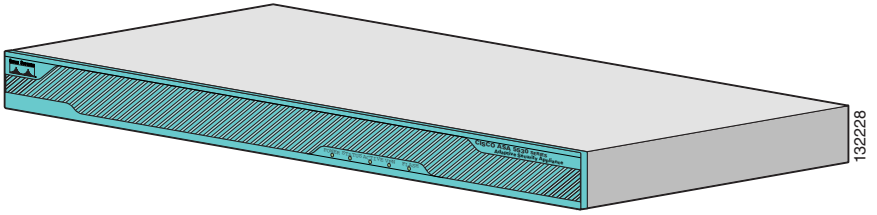
Quick Start Guide

Cisco ASA 5500 Series Adaptive Security Appliance Quick Start Guide

1 Verifying the Package Contents
2 Installing the Cisco ASA 5500 Series Adaptive Security Appliance
3 Configuring the Cisco ASA 5500 Series Adaptive Security Appliance
4 Common Configuration Scenarios
5 Optional SSM Setup and Configuration Procedures
6 Optional Maintenance and Upgrade Procedures

About the Cisco ASA 5500 Series Adaptive Security Appliance



The Cisco ASA 5500 series adaptive security appliance family delivers enterprise-class security for medium business-to-enterprise networks in a modular, purpose-built appliance. Its versatile one-rack unit (1RU) design supports up to 8 10/100/1000 Gigabit Ethernet interfaces (on the 5520 and 5540) and 1 10/100 Fast Ethernet Management interface, making it an excellent choice for businesses requiring a cost-effective, resilient security solution with demilitarized zone (DMZ) support. The optional 4GE SSM provides four ports, each with two interfaces, copper RJ-45 (Ethernet) and SFP for optical fiber connections. Part of the market-leading Cisco adaptive security appliance series, the Cisco ASA 5500 provides a wide range of integrated security services, hardware VPN acceleration, full intrusion prevention, award-winning high-availability and powerful remote management capabilities in an easy-to-deploy, high-performance solution.

About This Document

This document describes how to install and configure the Cisco ASA 5510, 5520, and 5540 adaptive security appliance to be used in VPN, DMZ, remote-access, and intrusion protection deployments.

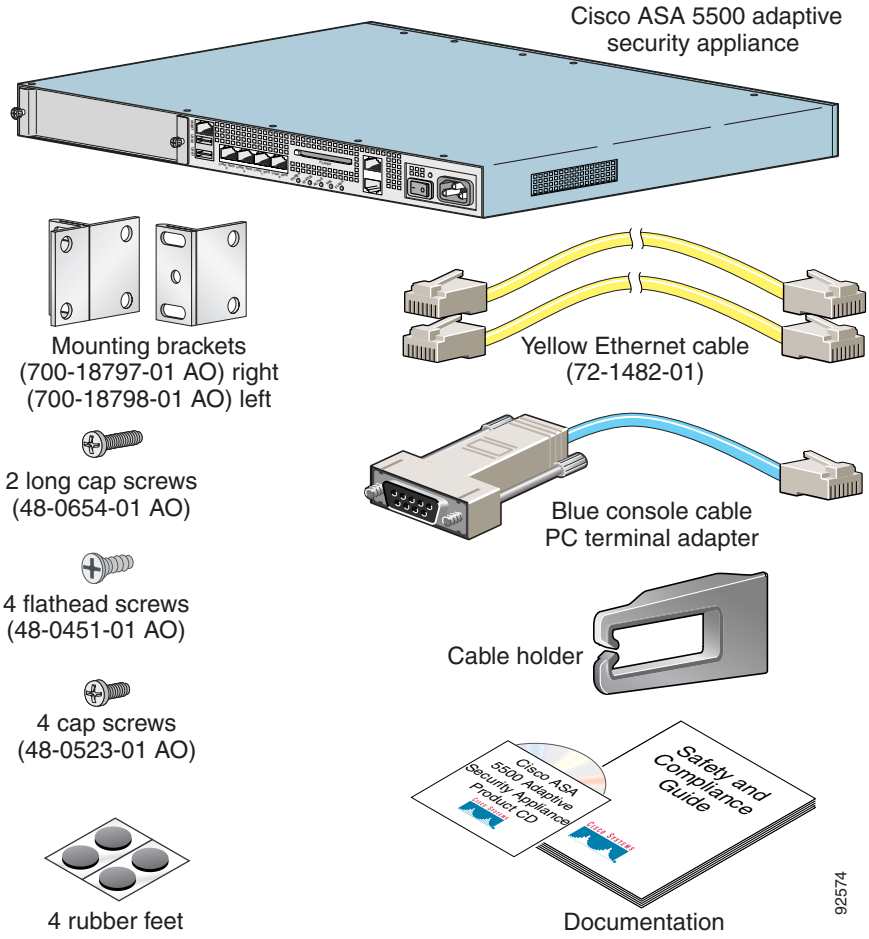
When you have completed the procedures outlined in this document, the adaptive security appliance will be running a robust VPN, DMZ, or remote-access configuration appropriate for most deployments. The document provides only enough information to get the adaptive security appliance up and running with a basic configuration.

For more information, see the following documentation:

- *Cisco ASA 5500 Series Release Notes*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance Command Reference*
- *Cisco Security Appliance Logging Configuration and System Log Messages*

1 Verifying the Package Contents

Verify the contents of the packing box to ensure that you have received all items necessary to install your Cisco ASA 5500 series adaptive security appliance.


Cisco ASA 5500 adaptive security appliance
Mounting brackets (700-18797-01 AO) right (700-18798-01 AO) left
Yellow Ethernet cable (72-1482-01)
2 long cap screws (48-0654-01 AO)
Blue console cable PC terminal adapter
4 flathead screws (48-0451-01 AO)
Cable holder
4 cap screws (48-0523-01 AO)
Cisco ASA 5500 Adaptive Security Appliance Product CD
Safety and Compliance Guide
4 rubber feet
Documentation
92574

2 Installing the Cisco ASA 5500 Series Adaptive Security Appliance

Warning **This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.** Statement 1071

Caution Be sure to read the safety warnings in the *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series* and follow proper safety procedures when performing these steps.

Warning **To prevent bodily injury when mounting or servicing this unit in a rack, you must take special precautions to ensure that the system remains stable. The following guidelines are provided to ensure your safety:**

- **This unit should be mounted at the bottom of the rack if it is the only unit in the rack.**
- **When mounting this unit in a partially filled rack, load the rack from the bottom to the top with the heaviest component at the bottom of the rack.**
- **If the rack is provided with stabilizing devices, install the stabilizers before mounting or servicing the unit in the rack.** Statement 1006

Use the following guidelines when installing the adaptive security appliance in a rack:

- Allow clearance around the rack for maintenance.
- When mounting a device in an enclosed rack, ensure adequate ventilation. An enclosed rack should never be overcrowded. Each unit generates heat.
- When mounting a device in an open rack, make sure that the rack frame does not block the intake or exhaust ports.

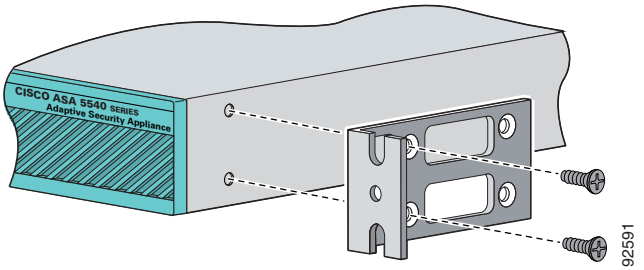
Warning **Before performing any of the following procedures, ensure that power is removed from the DC circuit. To ensure that all power is OFF, locate the circuit breaker on the panel board that services the DC circuit, switch the circuit breaker to the OFF position, and tape the switch handle of the circuit breaker in the OFF position.** Statement 7

Rack Mounting the Chassis

To rack mount the chassis, perform the following steps:

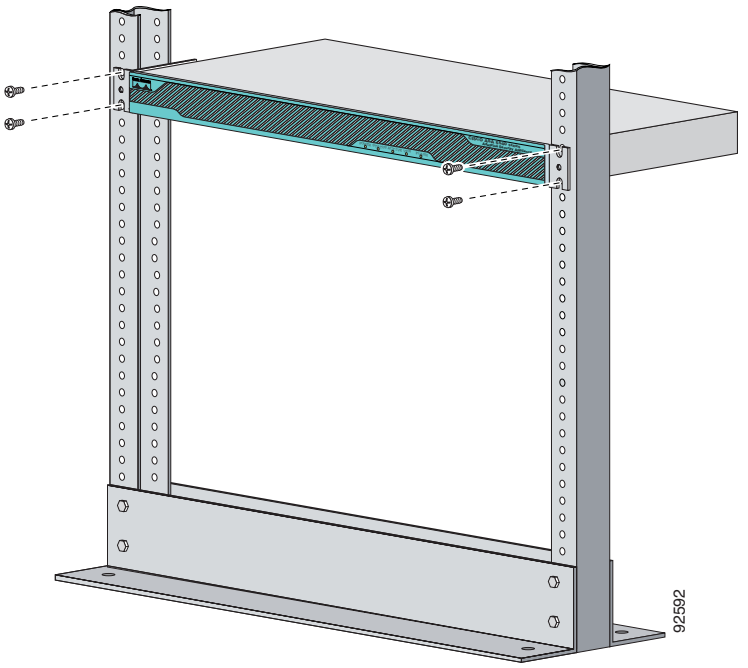
Step 1 Attach the rack-mount brackets to the chassis by using the supplied screws. Attach the brackets to the holes near the front or at the rear of the chassis. (See Figure 1.)

Figure 1 Installing the Brackets



Step 2 Attach the chassis to the rack by using the supplied screws. (See Figure 2.)

Figure 2 Rack Mounting the Chassis



Connecting the Interface Cables

To connect the interface cables, perform the following steps:

Step 1 Connect a computer or terminal to the adaptive security appliance for management access.

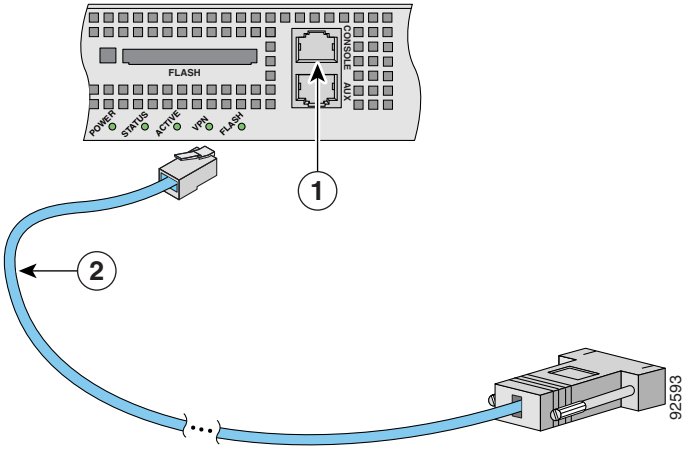
Note Before connecting a computer or terminal to the Console port, check the baud rate. The baud rate must match the default baud rate (9600 baud) of the console port on the adaptive security appliance. Set up the computer or terminal as follows: 9600 baud (default), 8 data bits, no parity, 1 stop bits, and FC=hardware.

Step 2 Locate the blue console cable from the accessory kit. The console cable has an RJ-45 connector on one end and a DB-9 connector on the other.

Step 3 Connect the RJ-45 connector of the blue console cable to the Console port on the rear panel of the adaptive security appliance. (See Figure 3.)

Step 4 Connect the DB-9 connector of the blue cable to the serial port on your computer or terminal.

Figure 3 Connecting the Chassis Console Cable



1	RJ-45 console port
2	RJ-45 to DB-9 serial console cable (null modem)

Note Alternatively, for management purposes, you can also connect an Ethernet cable to the adaptive security appliance MGMT port. The MGMT port is a Fast Ethernet interface designed for management traffic only and is specified as Management0/0. The MGMT port is similar to the Console port, but the MGMT port accepts only incoming traffic.

Step 5 Locate the yellow Ethernet cable in the accessory kit.

Step 6 Attach one end of the Ethernet cable to an Ethernet port and the other end to a network device, such as a router, switch, or hub.

Step 7 Attach the power cord to the adaptive security appliance and the power source.

Step 8 Power on the chassis.

3 Configuring the Cisco ASA 5500 Series Adaptive Security Appliance

This section describes the initial configuration of the adaptive security appliance. You can perform the configuration steps using either the browser-based Cisco Adaptive Security Device Manager (ASDM) or the command-line interface (CLI).

Note To use ASDM, you must have a DES license or a 3DES-AES license. For more information, see Obtaining DES and 3DES/AES Encryption Licenses, page 52.

About the Factory Default Configuration

Cisco adaptive security appliances are shipped with a factory-default configuration that enables quick startup. This configuration meets the needs of most small and medium business networking environments. By default, the adaptive security appliance is configured as follows:

- The inside (GigabitEthernet0/1) interface is configured with a default DHCP address pool.

  This configuration enables a client on the inside network to obtain a DHCP address from the adaptive security appliance in order to connect to the appliance. Administrators can then configure and manage the adaptive security appliance using ASDM.

- The outside (GigabitEthernet0/0) interface is used to connect to the public network and is configured to deny all inbound traffic.

  This configuration protects your inside network from unsolicited traffic.

Based on your network security policy, you should also consider configuring the adaptive security appliance to deny all ICMP traffic through the outside interface or any other interface that is necessary. You can configure this access control policy using the **icmp** command. For more information about the **icmp** command, see the *Cisco Security Appliance Command Reference*.

About the Adaptive Security Device Manager

The Adaptive Security Device Manager (ASDM) is a feature-rich graphical interface that enables you to manage and monitor the adaptive security appliance. Its web-based design provides secure access so that you can connect to and manage the adaptive security appliance from any location by using a web browser.

In addition to complete configuration and management capability, ASDM features intelligent wizards to simplify and accelerate the deployment of the adaptive security appliance.

To use ASDM, you must have a DES license or a 3DES-AES license. In addition, Java and JavaScript must be enabled in your web browser.

Cisco Adaptive Security Device Manager
Cisco Systems
Copyright © 2001 - 2005 Cisco Systems, Inc. All rights reserved.
104306

About Configuration from the Command-Line Interface

In addition to the ASDM web configuration tool, you can configure the adaptive security appliance by using the command-line interface. For more information, see the *Cisco Security Appliance Command Line Configuration Guide* and the *Cisco Security Appliance Command Reference*.

Using the Startup Wizard

ASDM includes a Startup Wizard to simplify the initial configuration of your adaptive security appliance. With a few steps, the Startup Wizard enables you to configure the adaptive security appliance so that it allows packets to flow securely between the inside network (GigabitEthernet0/1) and the outside network (GigabitEthernet0/0).

Before you launch the Startup Wizard, gather the following information:

- A unique hostname to identify the adaptive security appliance on your network.
- The IP addresses of your outside interface, inside interface, and any other interfaces.
- The IP addresses to use for NAT or PAT configuration.

- The IP address range for the DHCP server.

To use the Startup Wizard to set up a basic configuration for the adaptive security appliance, perform the following steps:

Step 1 If you have not already done so, connect the MGMT interface to a switch or hub by using the Ethernet cable. To this same switch, connect a PC for configuring the adaptive security appliance.

Step 2 Configure your PC to use DHCP (to receive an IP address automatically from the adaptive security appliance), or assign a static IP address to your PC by selecting an address out of the 192.168.1.0 network. (Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1.)

Note The MGMT interface of the adaptive security appliance is assigned 192.168.1.1 by default, so this address is unavailable.

Step 3 Check the LINK LED on the MGMT interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub turn solid green.

Step 4 Launch the Startup Wizard.

a. On the PC connected to the switch or hub, launch an Internet browser.

b. In the address field of the browser, enter this URL: **https://192.168.1.1/**.

Note The adaptive security appliance ships with a default IP address of 192.168.1.1. Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.

Step 5 In the dialog box that requires a username and password, leave both fields empty. Press **Enter**.

Step 6 Click **Yes** to accept the certificates. Click **Yes** for all subsequent authentication and certificate dialog boxes.

ASDM starts.

Step 7 From the Wizards menu at the top of the ASDM window, choose Startup Wizard.

Step 8 Follow the instructions in the Startup Wizard to set up your adaptive security appliance. For information about any field in the Startup Wizard, click **Help** at the bottom of the window.

4 Common Configuration Scenarios

This section provides configuration examples for three common deployments of the adaptive security appliance:

- Hosting a web server on a DMZ network
- Establishing remote-access VPN connections so that off-site clients can establish secure communications with the internal network
- Establishing a site-to-site VPN connection with other business partners or remote offices

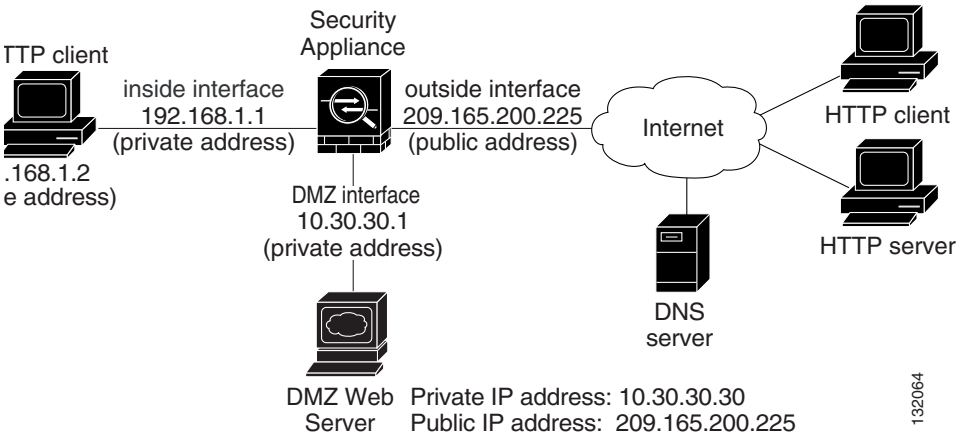
Use these scenarios as a guide when you set up your network. Substitute your own network addresses and apply additional policies as needed.

Scenario 1: DMZ Configuration

A demilitarized zone (DMZ) is a separate network located in the neutral zone between a private (inside) network and a public (outside) network. This example network topology is similar to most DMZ implementations of the adaptive security appliance. The web server is on the DMZ interface, and HTTP clients from both the inside and outside networks can access the web server securely.

In Figure 4, an HTTP client (10.10.10.10) on the inside network initiates HTTP communications with the DMZ web server (10.30.30.30). HTTP access to the DMZ web server is provided for all clients on the Internet; all other communications are denied. The network is configured to use an IP pool of addresses between 10.30.30.50 and 10.30.30.60. (The IP pool is the range of IP addresses available to the DMZ interface.)

Figure 4 Network Layout for DMZ Configuration Scenario



Because the DMZ web server is located on a private DMZ network, it is necessary to translate its private IP address to a public (routable) IP address. This public address allows external clients to access the DMZ web server in the same way that they access any server on the Internet.

The DMZ configuration scenario shown in Figure 4 provides two routable IP addresses that are publicly available: one for the outside interface (209.165.200.225) of the adaptive security appliance, and one for the public IP address of the DMZ web server (209.165.200.226). The following procedure describes how to use ASDM to configure the adaptive security appliance for secure communications between HTTP clients and the web server.

In this DMZ scenario, the adaptive security appliance already has an outside interface configured, called **dmz**. Set up the adaptive security appliance interface for your DMZ by using the Startup Wizard. Ensure that the security level is set between 0 and 100. (A common choice is 50.)

Information to Have Available

Before you begin this configuration procedure, gather the following information:

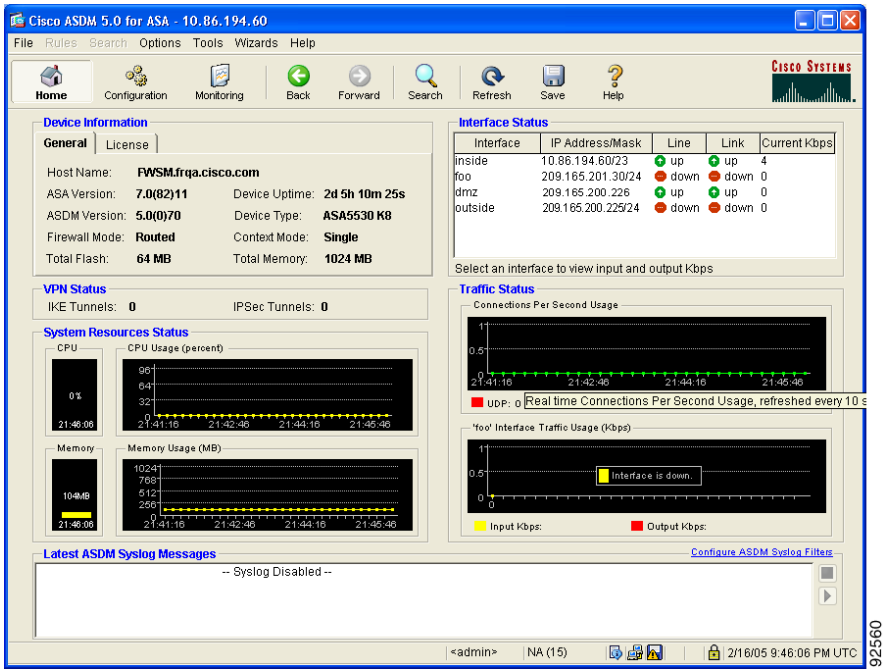
- Internal IP addresses of the servers inside the DMZ that you want to make available to clients on the public network (in this scenario, a web server).
- External IP addresses to be used for servers inside the DMZ. (Clients on the public network will use the external IP address to access the server inside the DMZ.)
- Client IP address to substitute for internal IP addresses in outgoing traffic. (Outgoing client traffic will appear to come from this address so that the internal IP address is not exposed.)

Step 1: Configure IP Pools for Network Translations.

For an inside HTTP client (10.10.10.10) to access the web server on the DMZ network (10.30.30.30), it is necessary to define a pool of IP addresses (10.30.30.50–10.30.30.60) for the DMZ interface. Similarly, an IP pool for the outside interface (209.165.200.225) is required for the inside HTTP client to communicate with any device on the public network. Use ASDM to manage IP pools efficiently and to facilitate secure communications between protected network clients and devices on the Internet.

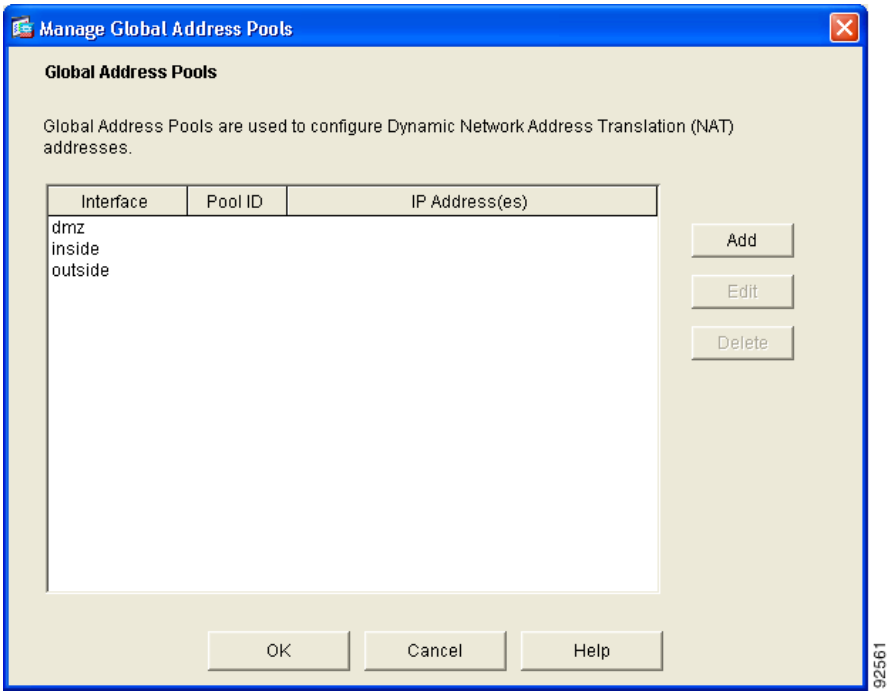
1. Launch ASDM by entering this factory default IP address in the address field of a web browser: **https://192.168.1.1/admin/**.

Note Remember to add the "**s**" in "**https**" or the connection fails. HTTPS (HTTP over SSL) provides a secure connection between your browser and the adaptive security appliance.



2. Click **Configuration** at the top of the ASDM window.
3. Choose the **NAT** feature on the left side of the ASDM window.

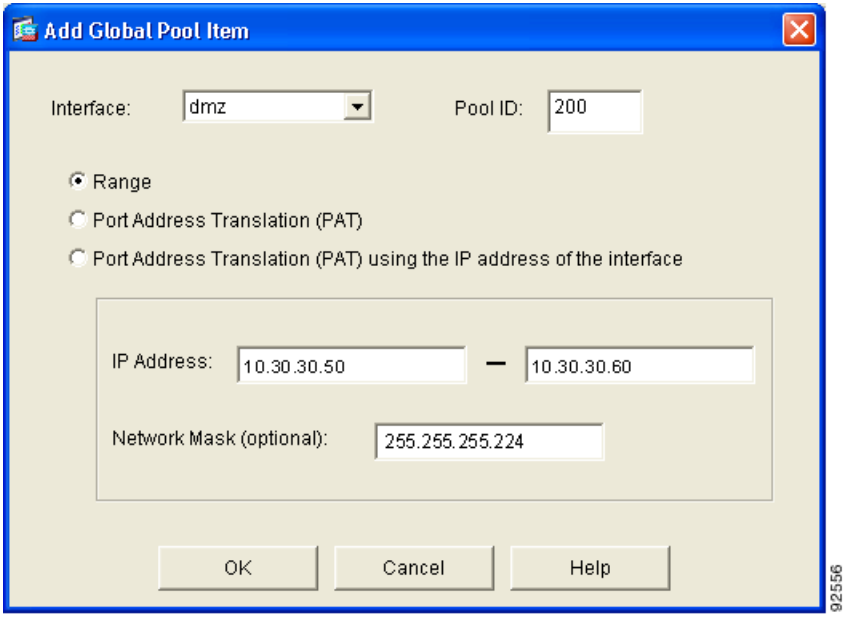
4. Click **Manage Pools** at the bottom of the ASDM window. The Manage Global Address Pools dialog box appears, allowing you to add or edit global address pools.



Note For most configurations, global pools are added to the less secure, or public, interfaces.

5. In the Manage Global Address Pools dialog box:
   a. Choose the **dmz** interface (configured using the Startup Wizard before beginning this procedure).

b. Click **Add**. The Add Global Pool Item dialog box appears.

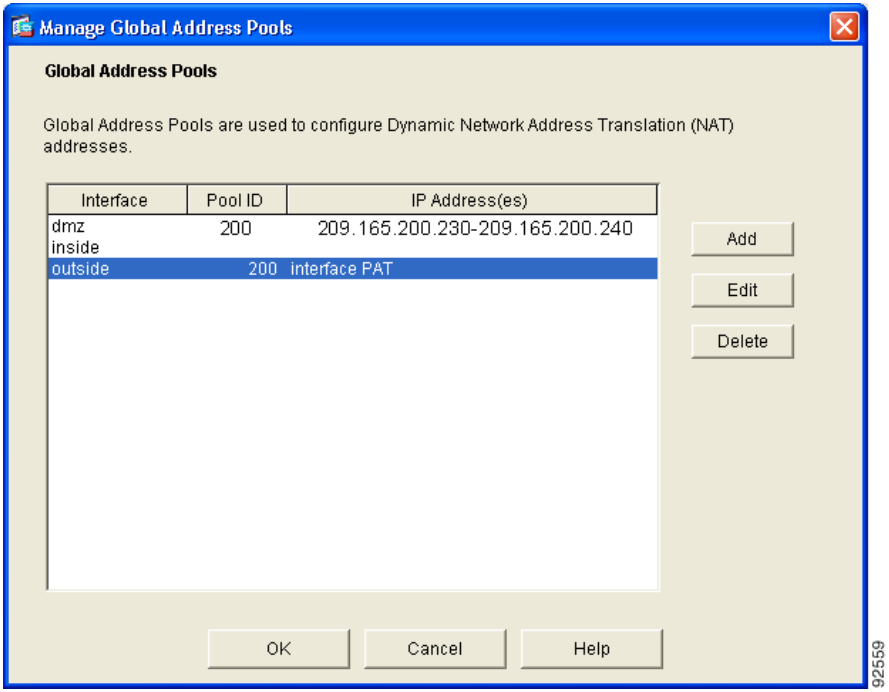


6. In the Add Global Pool Item dialog box:
   a. Choose **dmz** from the **Interface** drop-down menu.
   b. Click **Range** to enter the IP address range.
   c. Enter the range of IP addresses for the DMZ interface. In this scenario, the range is 209.165.200.230 to 209.165.200.240.
   d. Enter a unique Pool ID. In this scenario, the Pool ID is 200.
   e. Click **OK** to return to the Manage Global Address Pools dialog box.

Note You can also choose **Port Address Translation (PAT)** or **Port Address Translation (PAT) using the IP address of the interface** if there are limited IP addresses available for the DMZ interface.

7. In the Manage Global Address Pools dialog box:
   a. Choose the **outside** interface.
   b. Click **Add**.

8. When the Add Global Pool Item dialog box appears:
   a. Choose **outside** from the **Interface** drop-down menu.
   b. Click **Port Address Translation (PAT) using the IP address of the interface.**
   c. Assign the same Pool ID for this pool as you did in Step 6d. (For this scenario, the Pool ID is 200.)
   d. Click **OK**. The displayed configuration should be similar to the following:



9. Confirm that the configuration values are correct, then:
   a. Click **OK**.
   b. Click **Apply** in the main ASDM window.

Note Because there are only two public IP addresses available, with one reserved for the DMZ server, all traffic initiated by the inside HTTP client exits the adaptive security appliance using the outside interface IP address. This configuration allows traffic from the inside client to be routed to and from the Internet.

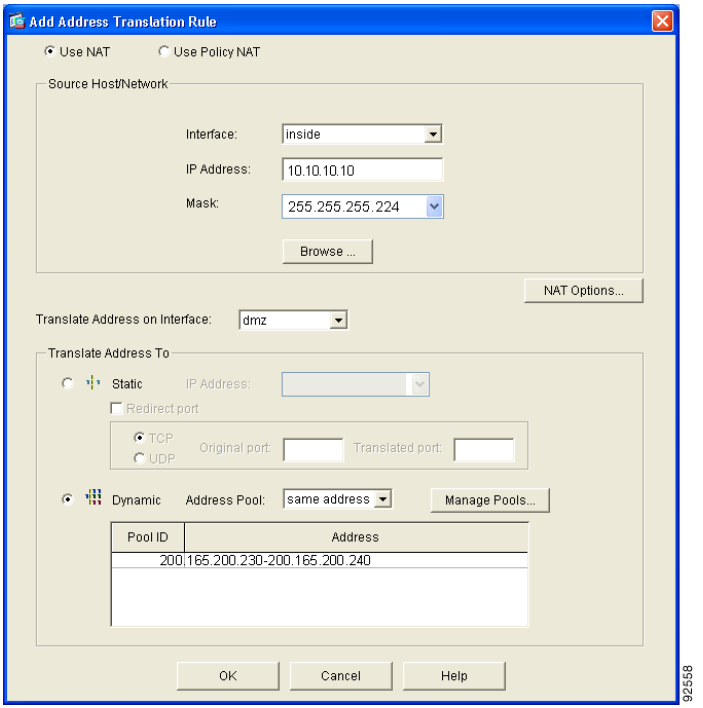
Step 2: Configure Address Translations on Private Networks.

Network Address Translation (NAT) replaces the source IP addresses of network traffic exchanged between two interfaces on the adaptive security appliance. This translation permits routing through the public networks while preventing internal IP addresses from being exposed on the public networks.

Port Address Translation (PAT) is an extension of the NAT function that allows several hosts on a private network to map into a single IP address on the public network. PAT is essential for small and medium businesses that have a limited number of public IP addresses available to them.

To configure NAT between the inside interface and the DMZ interface for the inside HTTP client, perform the following steps starting from the main ASDM page:

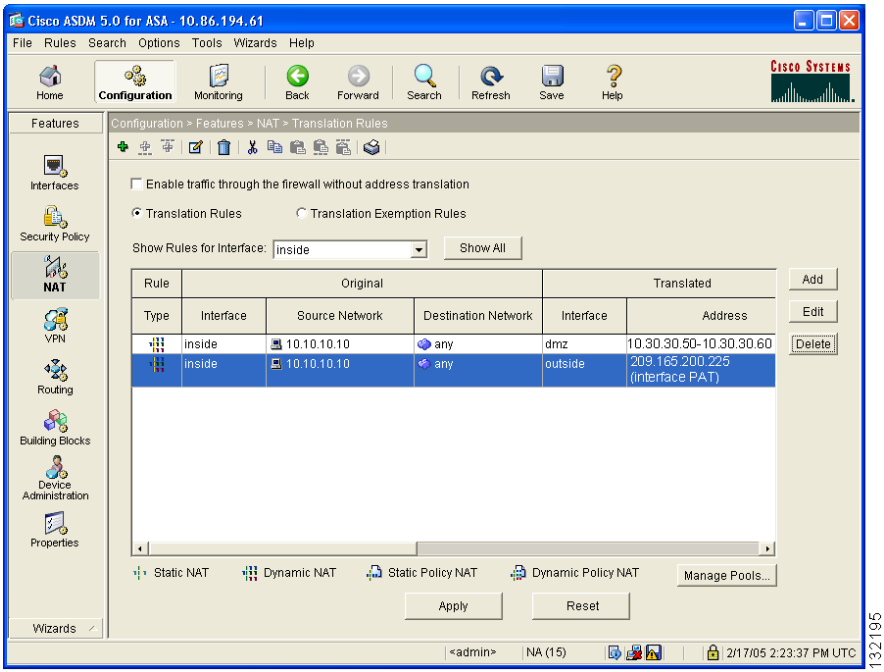
1. Click **Configuration** at the top of the ASDM window.
2. Choose the **NAT** feature on the left side of the ASDM window.
3. Click **Translation Rules**, and then click **Add** at the right side of the ASDM page.
4. In the Add Address Translation Rule dialog box, make sure that **Use NAT** is selected, and then choose the **inside** interface.



5. Enter the IP address of the inside client. In this scenario, the IP address is **10.10.10.10**.

6. Choose **255.255.255.224** from the **Mask** drop-down menu.
7. Select the DMZ interface from the **Translate Address on Interface** drop-down menu.
8. Click **Dynamic** in the **Translate Address To** section.
9. Choose **200** from the **Address Pools** drop-down menu for the Pool ID.
10. Click **OK**.
11. A dialog box appears asking if you want to proceed. Click **Proceed**.
12. On the NAT Translation Rules page, check the displayed configuration for accuracy.
13. Click **Apply** to complete the adaptive security appliance configuration changes.

The displayed configuration should be similar to the following:

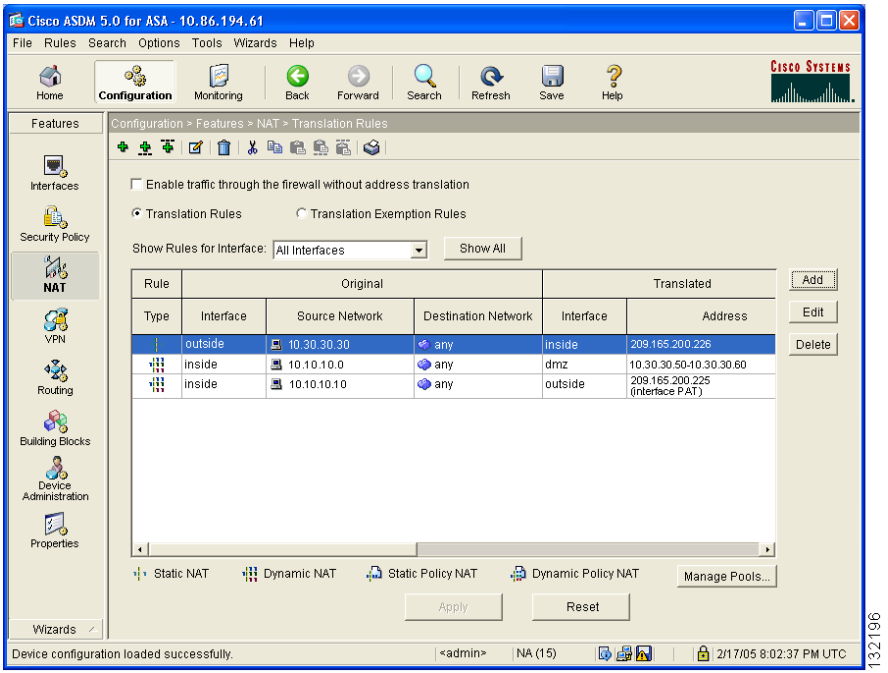


Step 3: Configure External Identity for the DMZ Web Server.

The DMZ web server needs to be easily accessible by all hosts on the Internet. This configuration requires translating the web server's IP address so that it appears to be located on the Internet, enabling outside HTTP clients to access it unaware of the adaptive security appliance. Complete the following steps to map the web server IP address (10.30.30.30) statically to a public IP address (209.165.200.225):

1. Click **Configuration** at the top of the ASDM window.
2. Choose the **NAT** feature on the left side of the ASDM window.
3. Click **Translation Rules,** then click **Add** at the right side of the page.
4. Choose the outside **dmz** interface from the drop-down list of interfaces.
5. Enter the **IP address** (10.30.30.30) for the web server.
6. Choose **255.255.255.224** from the **Mask** drop-down menu, then click **Static**.
7. Enter the external IP address (209.165.200.226) for the web server. Then click **OK**.
8. Verify the values that you entered, then click **Apply**.

The displayed configuration should be similar to the following:



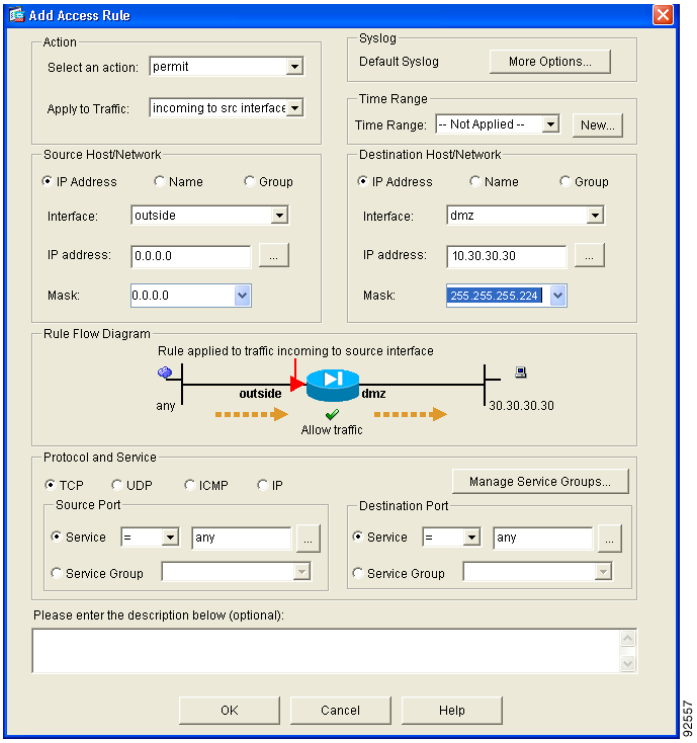
Step 4: Provide HTTP Access to the DMZ Web Server.

By default, the adaptive security appliance denies all traffic coming in from the public network. You must create access control rules on the adaptive security appliance to allow specific traffic types from the public network through the adaptive security appliance to resources in the DMZ.

To configure an access control rule that allows HTTP traffic through the adaptive security appliance so that any client on the Internet can access a web server inside the DMZ, perform the following steps:

1. In the ASDM window:
   a. Click **Configuration**.
   b. Choose **Security Policy** on the left side of the ASDM screen.
   c. In the table, click **Add**.
2. In the Add Access Rule dialog box:
   a. Under **Action**, choose **permit** from the drop-down menu to allow traffic through the adaptive security appliance.
   b. Under Source Host/Network, click **IP Address**.
   c. Choose **outside** from the **Interface** drop-down menu.
   d. Enter the IP address of the Source Host/Network information. (Use 0.0.0.0 to allow traffic originating from any host or network.)
   e. Under Destination Host/Network, click **IP Address**.
   f. Choose the **dmz** interface from the **Interface** drop-down menu.
   g. In the IP address field, enter the IP address of the destination host or network, such as a web server. (In this scenario, the IP address of the web server is 10.30.30.30.)
   h. Choose **255.255.255.224** from the **Mask** drop-down menu.

Note Alternatively, you can select the Hosts/Networks in both cases by clicking the respective **Browse** buttons.



3. Specify the type of traffic that you want to permit.

Note HTTP traffic is always directed from any TCP source port number toward a fixed destination TCP port number 80.

   a. Click **TCP** under Protocol and Service.
   b. Under Source Port, choose "**=**" (equal to) from the **Service** drop-down menu.
   c. Click the button labeled with ellipses (**...**), scroll through the options, and then choose **Any**.
   d. Under Destination Port, choose "**=**" (equal to) from the **Service** drop-down menu.
   e. Click the button labeled with ellipses (**...**), scroll through the options, and then select **HTTP**.

f. Click **OK**.

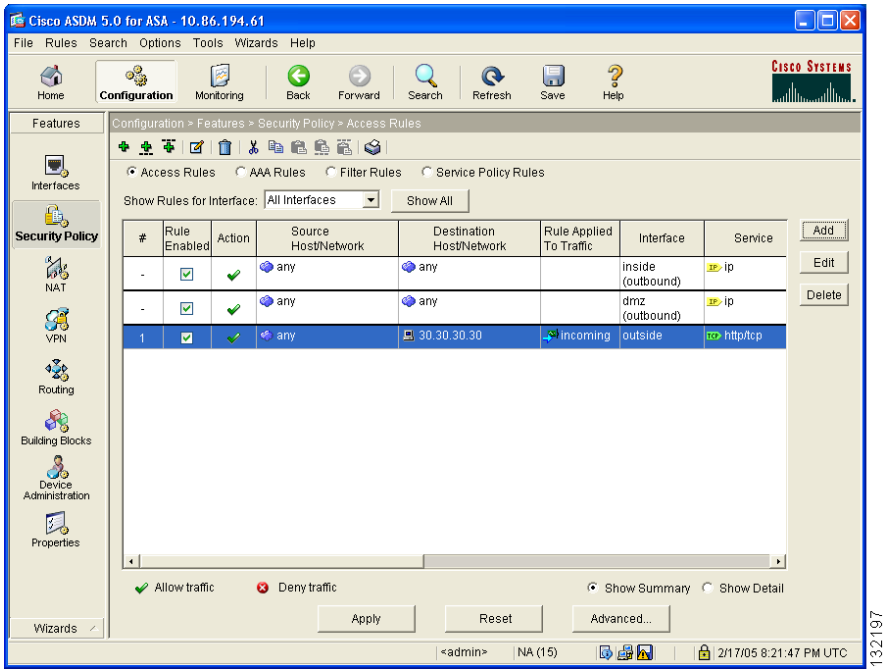
Note For additional features, such as logging system messages by ACL, click **More Options** at the top at the top of the screen. You can provide a name for the access rule in the dialog box at the bottom.

g. Verify that the information you entered is accurate, and then click **OK**.

Note Although the destination address specified is the private address of the DMZ web server (10.30.30.30), HTTP traffic from any host on the Internet destined for 209.165.200.225 is permitted through the adaptive security appliance. The address translation (10.30.30.30 = 209.165.200.225) allows the traffic to be permitted.

h. Click **Apply** in the main window.

The displayed configuration should be similar to the following:


Cisco ASDM 5.0 for ASA - 10.86.194.61
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Cisco Systems
Features
Configuration > Features > Security Policy > Access Rules
Interfaces
Security Policy
NAT
VPN
Routing
Building Blocks
Device Administration
Properties
Wizards
Access Rules AAA Rules Filter Rules Service Policy Rules
Show Rules for Interface: All Interfaces Show All
Rule Enabled Action Source Host/Network Destination Host/Network Rule Applied To Traffic Interface Service
- any any inside (outbound) ip
- any any dmz (outbound) ip
1 any 30.30.30.30 Incoming outside http/tcp
Add Edit Delete
Allow traffic Deny traffic Show Summary Show Detail
Apply Reset Advanced...
<admin> NA (15) 2/17/05 8:21:47 PM UTC
132197

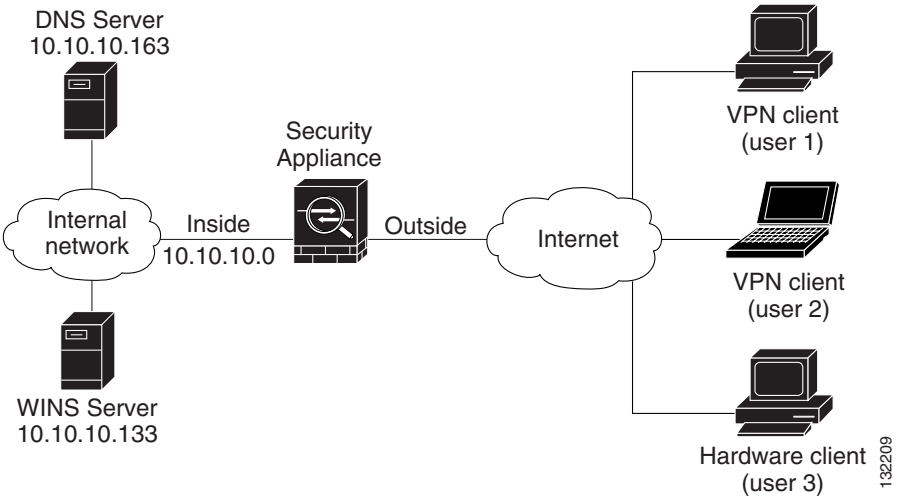
The HTTP clients on the private and public networks can now access the DMZ web server securely.

Scenario 2: Remote Access VPN

A remote-access Virtual Private Network (VPN) enables you to provide secure access to off-site users. ASDM enables you to configure the adaptive security appliance to create secure connections, or tunnels, across the Internet.

Figure 5 shows an adaptive security appliance configured to accept requests from and establish secure connections with VPN clients over the Internet.

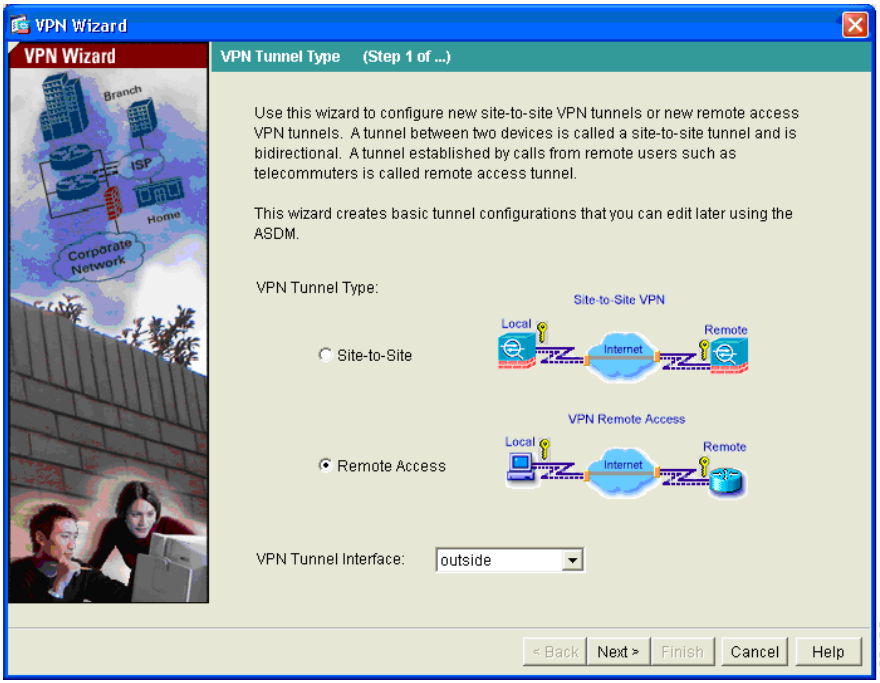
Figure 5 Network Layout for Remote Access VPN Scenario



The ASDM VPN Wizard enables you to configure the adaptive security appliance as a remote access VPN headend device in a series of simple steps.

Step 1: Configure the adaptive security appliance for remote access VPN.

1. Launch ASDM by entering the factory default IP address in the address field of a web browser: **https://192.168.1.1/admin/**.
2. In the main ASDM page, choose the VPN Wizard option from the **Wizards** drop-down menu. The VPN Wizard Step 1 window appears.

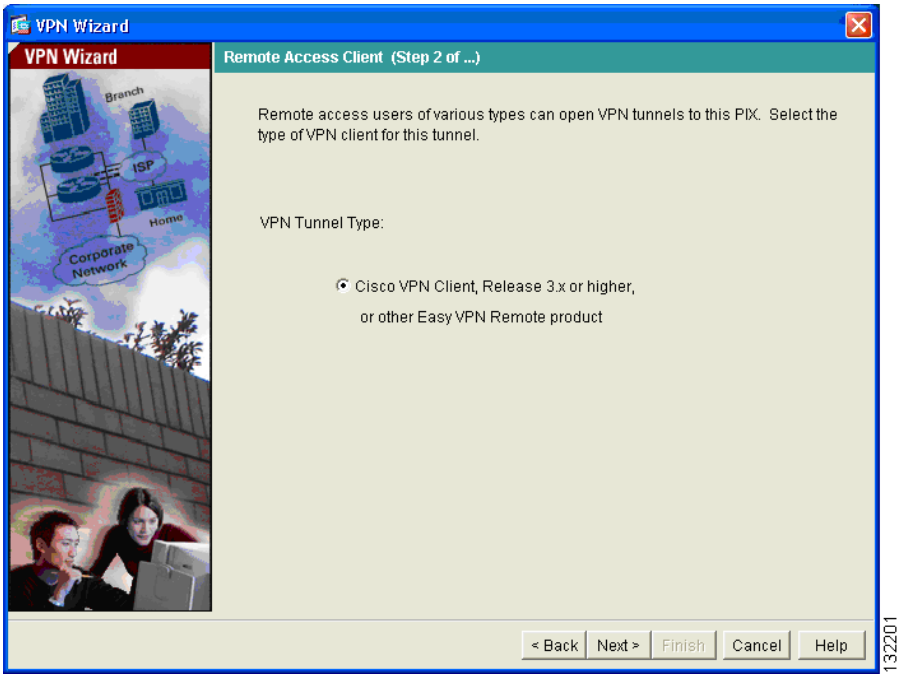


3. In Step 1 of the VPN Wizard, complete the following steps:
   a. Select the Remote Access VPN option.
   b. From the drop-down menu, choose **outside** as the enabled interface for the incoming VPN tunnels.
   c. Click **Next** to continue.

Step 2: Select VPN clients.

1. In Step 2 of the VPN Wizard, click the radio button to allow remote access users to connect to the adaptive security appliance using either a Cisco VPN client or any other Easy VPN Remote products.

Note Although there is currently only one selection on this screen, it is set up so that other tunnel types can be enabled easily as they become available.

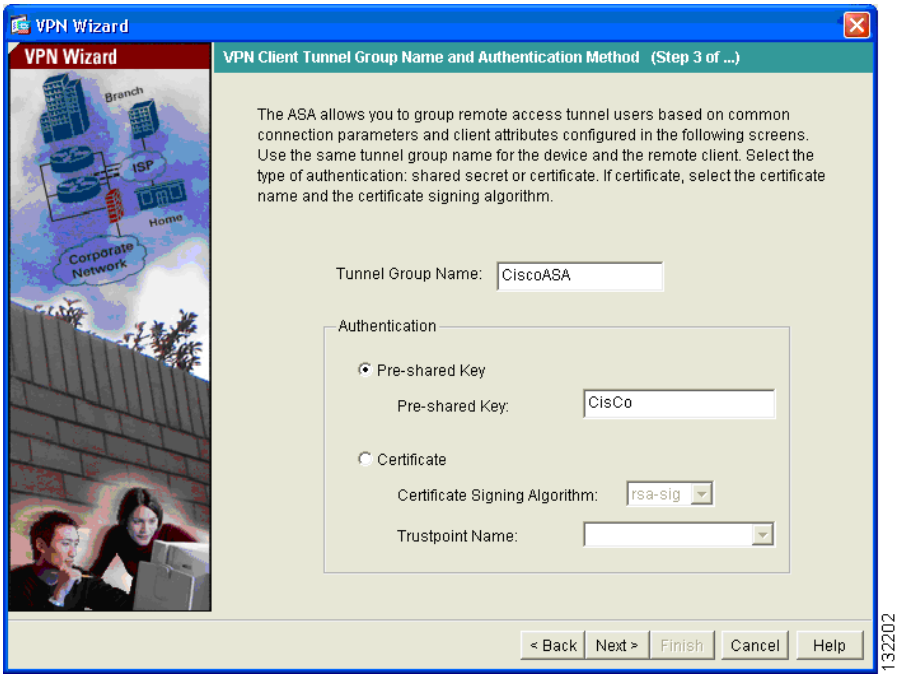


2. Click **Next** to continue.

Step 3: Specify the VPN tunnel group name and authentication method.

In Step 3 of the VPN Wizard, complete the following steps:

1. Enter a Tunnel Group Name (such as "CiscoASA") for the set of users that use common connection parameters and client attributes.


VPN Wizard
VPN Wizard
VPN Client Tunnel Group Name and Authentication Method (Step 3 of ...)
Branch
ISP
Home
Corporate Network
The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the following screens. Use the same tunnel group name for the device and the remote client. Select the type of authentication: shared secret or certificate. If certificate, select the certificate name and the certificate signing algorithm.
Tunnel Group Name: CiscoASA
Authentication
Pre-shared Key
Pre-shared Key: CisCo
Certificate
Certificate Signing Algorithm: rsa-sig
Trustpoint Name:
< Back
Next >
Finish
Cancel
Help
132202

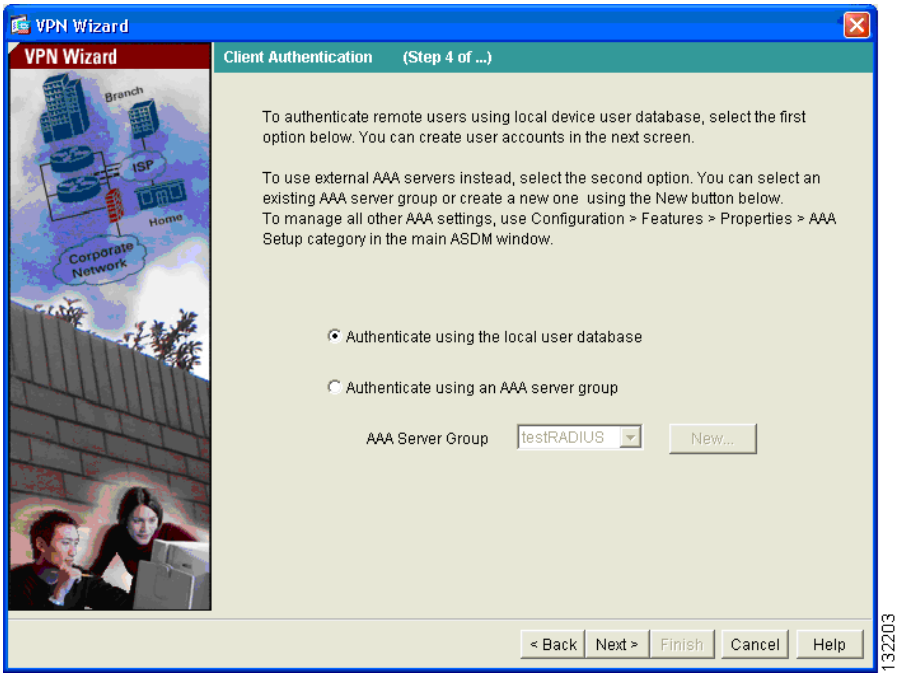
2. Specify the type of authentication that you want to use by performing one of the following steps:
   - To use static pre-shared keys for authentication, click **Pre-Shared Key**, and enter a key (such as "CisCo").
   - To use digital certificates for authentication, click **Certificate**, choose the Certificate Signing Algorithm (rsa-sig/dsa-sig) from the drop-down menu, and then choose a pre-configured trustpoint name from the drop-down menu.
3. Click **Next** to continue.

Step 4: Specify a user authentication method.

Users can be authenticated either by a local authentication database or by using external authentication, authorization, and accounting (AAA) servers (RADIUS, TACACS+, SDI, NT, and Kerberos).

In Step 4 of the VPN Wizard, complete the following steps:

1. Click the appropriate radio button to specify the type of user authentication that you want to use:
   - A local authentication database
   - An external AAA server group
2. Select a preconfigured server group from the drop down list, or click **New** to add a new server group.

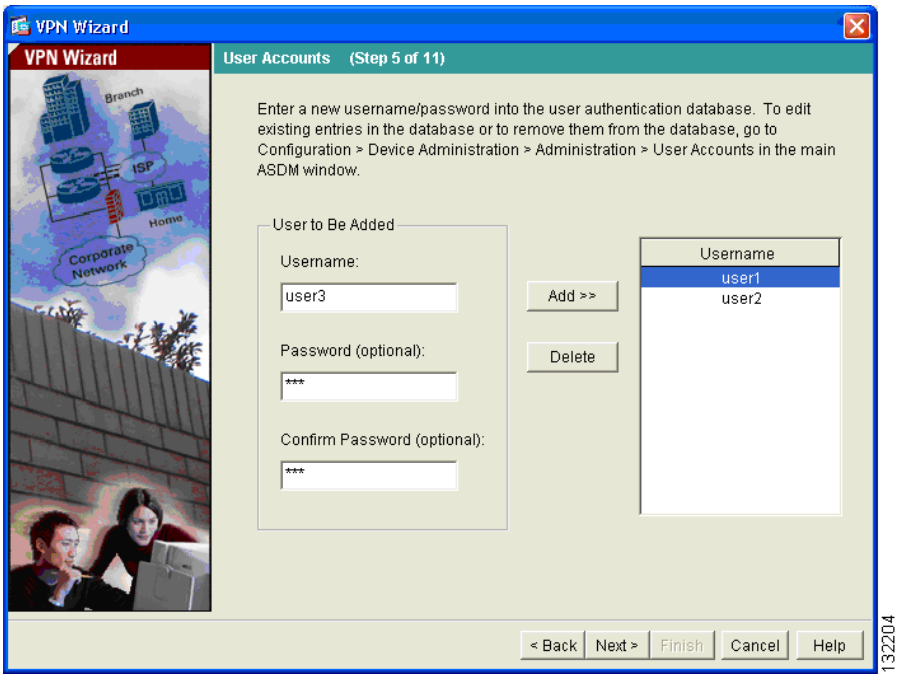

VPN Wizard
VPN Wizard
Client Authentication (Step 4 of ...)
Branch
ISP
Home
Corporate Network
To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next screen.
To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below.
To manage all other AAA settings, use Configuration > Features > Properties > AAA Setup category in the main ASDM window.
Authenticate using the local user database
Authenticate using an AAA server group
AAA Server Group
testRADIUS
New...
< Back
Next >
Finish
Cancel
Help
132203

3. Click **Next** to continue.

Step 5: Configure user accounts, if necessary.

If you chose to authenticate users with a local user database, create individual user accounts in Step 5 of the VPN Wizard.

1. To add a new user, enter a username and password, then click **Add**.



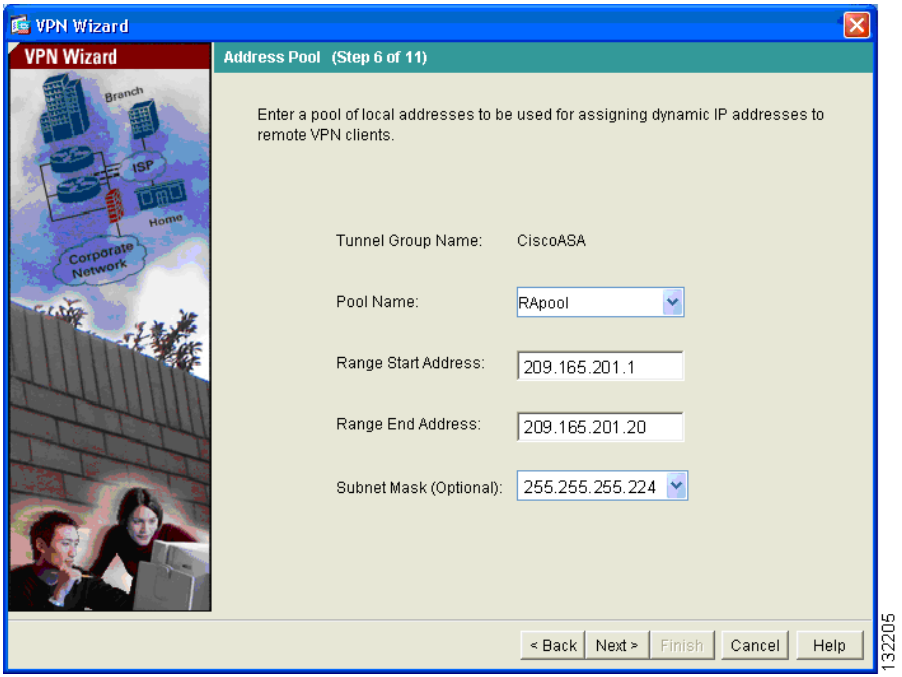
2. When you have finished adding new users, click **Next** to continue.

Step 6: Configure address pools.

For remote clients to gain access to your network, it is necessary to configure a pool of IP addresses that can be assigned to remote VPN clients as they are successfully connected. In this scenario, the pool is configured to use the range of IP addresses 209.165.201.1 to 209.166.201.20.

To configure an address pool, perform the following steps:

1. Enter a pool name, or choose a pre-configured pool from the drop down list.
2. Enter the start of the range of IP addresses to be used in the pool.
3. Enter the end of the range of IP addresses to be used in the pool.
4. Enter the subnet mask, or select a pre-configured value from the drop down list.



5. Click **Next** to continue.

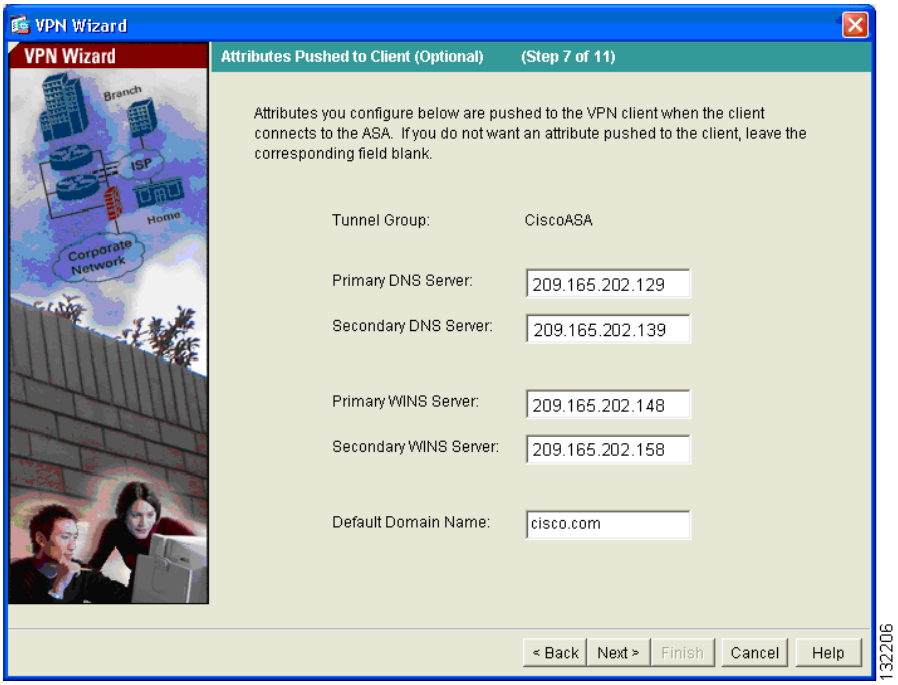
Step 7: Configure client attributes.

To access your network, each remote access client needs basic network configuration information, such as which DNS and WINS servers to use and the default domain name. Rather than configuring each remote client individually, you can provide the client information to ASDM. The adaptive security appliance pushes this information to the remote client when a connection is established.

Ensure that you specify the correct values, or remote clients will not be able to use DNS names for resolution or use Windows networking.

In Step 7 of the VPN Wizard, perform the following steps:

1. Enter the network configuration information to be used by remote clients.



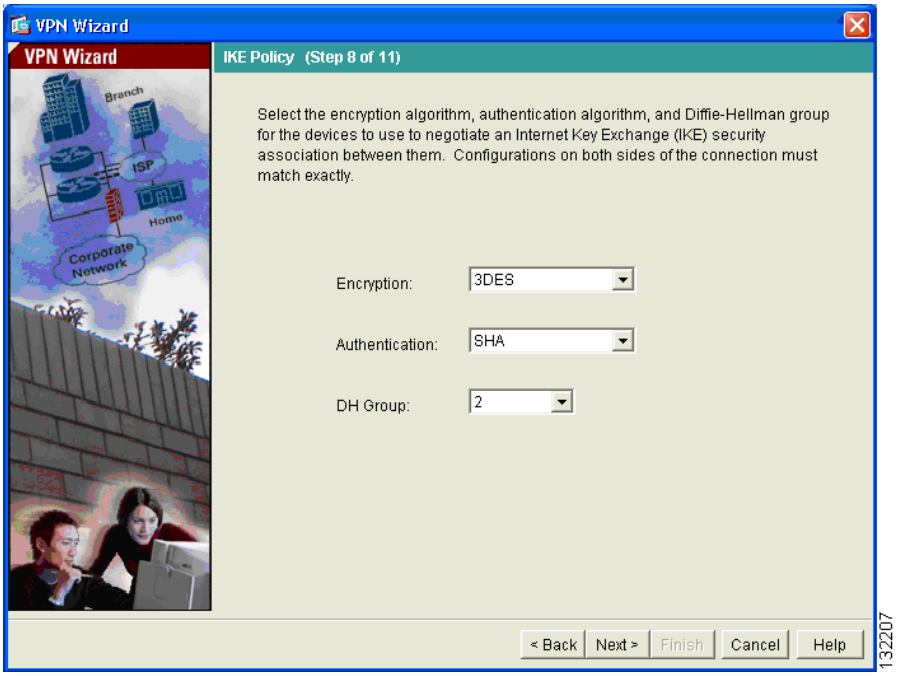
2. Click **Next** to continue.

Step 8: Configure the IKE Policy.

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels.

To specify the IKE policy, perform the following steps:

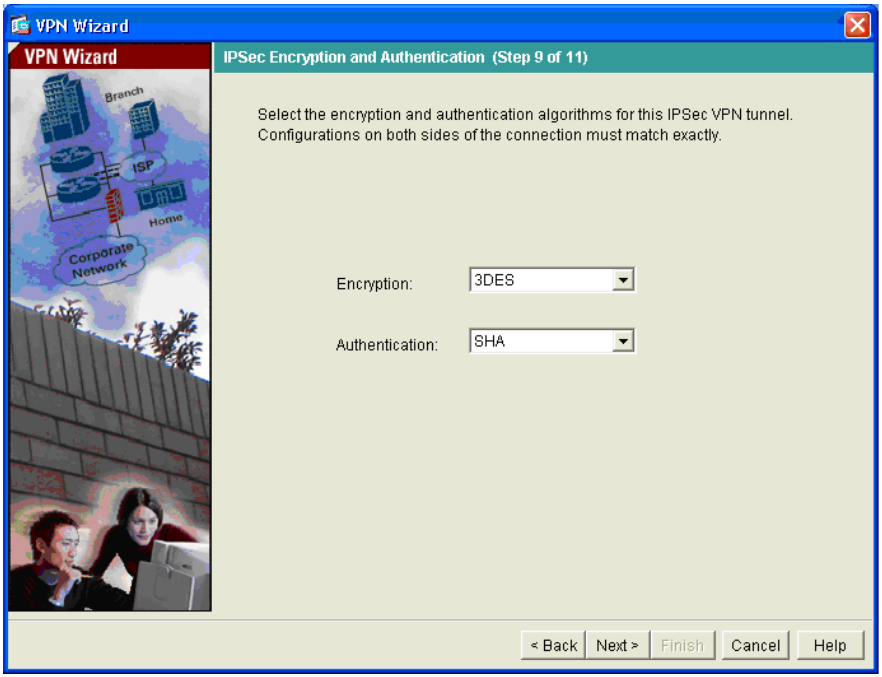
1. Select the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5/7) used by the adaptive security appliance during an IKE security association.



2. Click **Next** to continue.

Step 9: Configure IPSec Encryption and Authentication parameters.

1. Choose the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA).



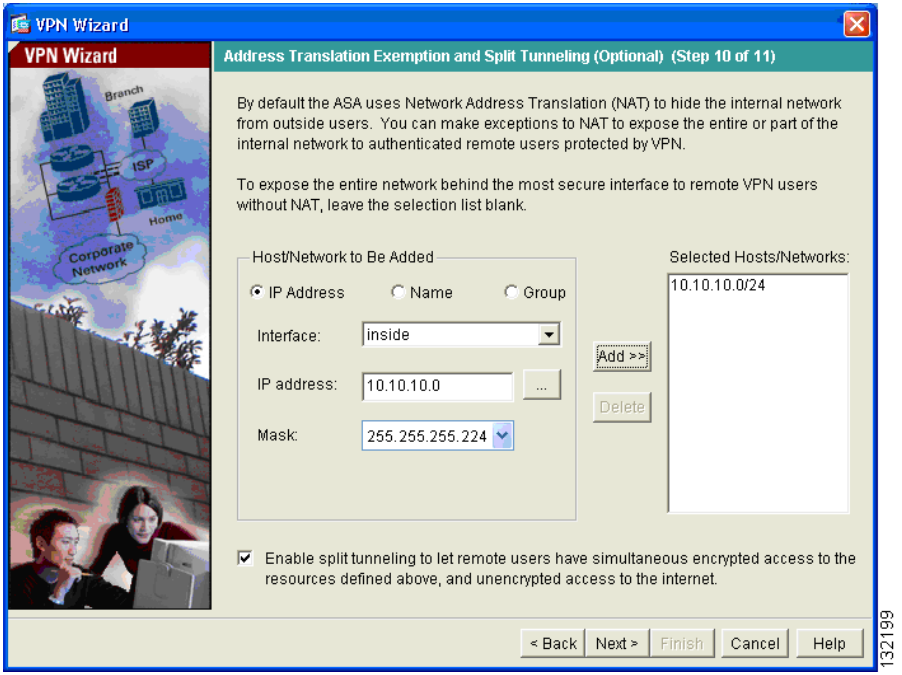
2. Click **Next** to continue.

Step 10: Address translation exception and split tunneling.

The adaptive security appliance uses Network Address Translation (NAT) to prevent internal IP addresses from being exposed externally. You can make exceptions to this network protection by identifying local hosts and networks that should be exposed to authenticated remote users. Specify the resources to be exposed by host or network IP address, by name, or by group. (In this scenario, the entire inside network 10.10.10.0 is exposed to all remote clients.)

In Step 10 of the VPN Wizard, add or remove hosts, groups, and networks dynamically from the Selected panel.

1. Click **Add** or **Delete**, as appropriate.

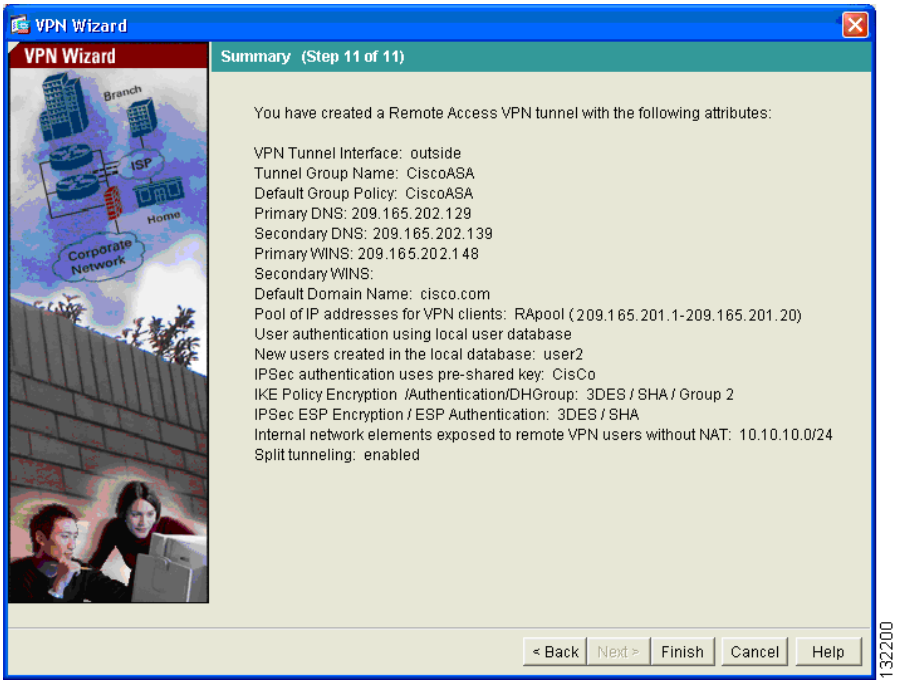

VPN Wizard
VPN Wizard
Address Translation Exemption and Split Tunneling (Optional) (Step 10 of 11)
Branch
ISP
Home
Corporate Network
By default the ASA uses Network Address Translation (NAT) to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN.
To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.
Host/Network to Be Added
IP Address
Name
Group
Interface:
inside
IP address:
10.10.10.0
Mask:
255.255.255.224
Add >>
Delete
Selected Hosts/Networks:
10.10.10.0/24
Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.
< Back
Next >
Finish
Cancel
Help
132199

Note Enable split tunneling by checking the radio button at the bottom of the screen. Split tunneling allows traffic outside the configured networks to be sent out directly to the Internet instead of over the encrypted VPN tunnel.

2. When you have finished specifying resources to expose to remote clients, click **Next** to continue.

Step 11: Verify the remote access VPN configuration.

Review the configuration attributes for the VPN tunnel you just created. The displayed configuration should be similar to the following:


VPN Wizard
VPN Wizard
Summary (Step 11 of 11)
Branch
ISP
Home
Corporate Network
You have created a Remote Access VPN tunnel with the following attributes:
VPN Tunnel Interface: outside
Tunnel Group Name: CiscoASA
Default Group Policy: CiscoASA
Primary DNS: 209.165.202.129
Secondary DNS: 209.165.202.139
Primary WINS: 209.165.202.148
Secondary WINS:
Default Domain Name: cisco.com
Pool of IP addresses for VPN clients: RApool (209.165.201.1-209.165.201.20)
User authentication using local user database
New users created in the local database: user2
IPSec authentication uses pre-shared key: CisCo
IKE Policy Encryption /Authentication/DHGroup: 3DES / SHA / Group 2
IPSec ESP Encryption / ESP Authentication: 3DES / SHA
Internal network elements exposed to remote VPN users without NAT: 10.10.10.0/24
Split tunneling: enabled
< Back
Next >
Finish
Cancel
Help
132200

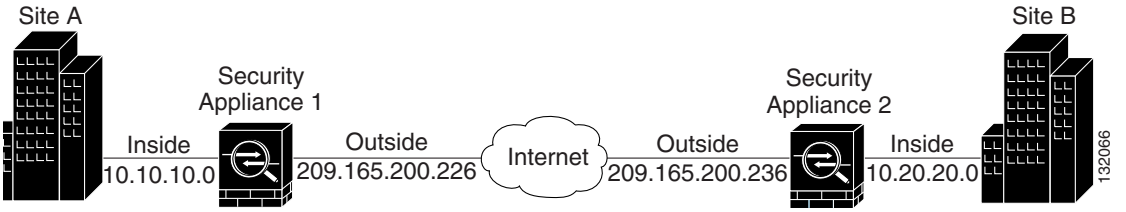
If you are satisfied with the configuration, click **Finish** to complete the Wizard and apply the configuration changes to the adaptive security appliance.

Scenario 3: Site-to-Site VPN Configuration

Site-to-site VPN (Virtual Private Networking) features provided by the adaptive security appliance enable businesses to extend their networks across low-cost public Internet connections to business partners and remote offices worldwide while maintaining their network security. A VPN connection enables you to send data from one location to another over a secure connection, or "tunnel," first by authenticating both ends of the connection, and then by automatically encrypting all data sent between the two sites.

Figure 6 shows an example VPN tunnel between two adaptive security appliances.

Figure 6 Network Layout for Site-to-Site VPN Configuration Scenario



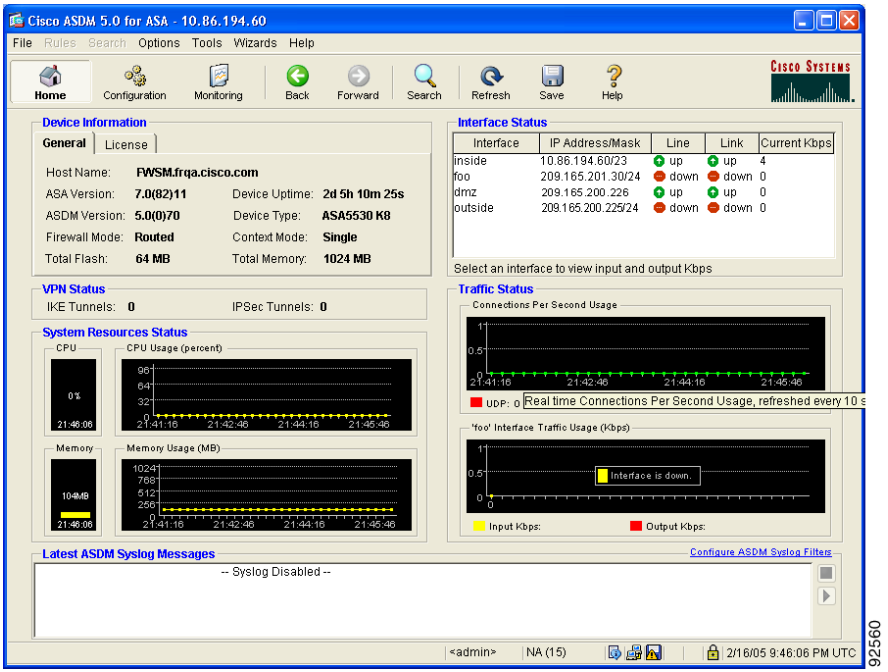
Creating a VPN site-to-site deployment such as the one in Figure 6 requires you to configure two adaptive security appliances, one on each side of the connection.

ASDM provides a configuration wizard to guide you through the process of configuring a site-to-site VPN.

Step 1: Configure the adaptive security appliance at the first site.

Configure the adaptive security appliance at the first site, which in this scenario is ASA security appliance 1, from this point forward referred to as ASA 1.

1. Launch ASDM by entering the factory default IP address in the address field of a web browser: **https://192.168.1.1/admin/**.



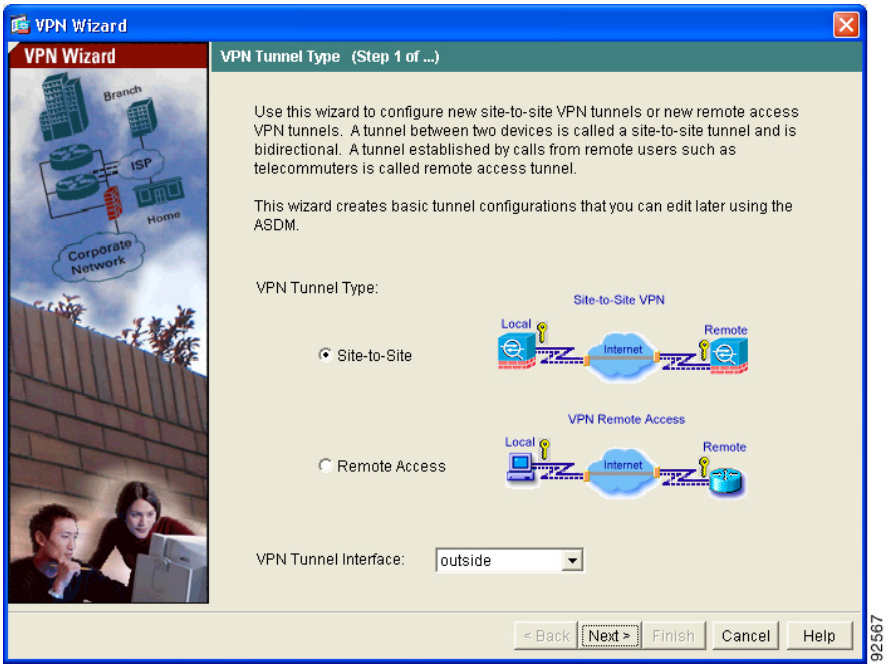
2. In the main ASDM page, choose the **VPN Wizard** option from the **Wizards** drop-down menu. ASDM opens the first VPN Wizard page.

   In the first page of the VPN Wizard, complete the following steps:

   a. Choose the **Site-to-Site VPN** option.

Note The Site-to-Site VPN option connects two IPSec security gateways, which can include adaptive security appliances, VPN concentrators, or other devices that support site-to-site IPSec connectivity.

b. From the drop-down menu, choose **outside** as the enabled interface for the current VPN tunnel.



c. Click **Next** to continue.

Step 2: Provide information about the VPN peer.

The VPN peer is the system on the other end of the connection that you are configuring, usually at a remote site.

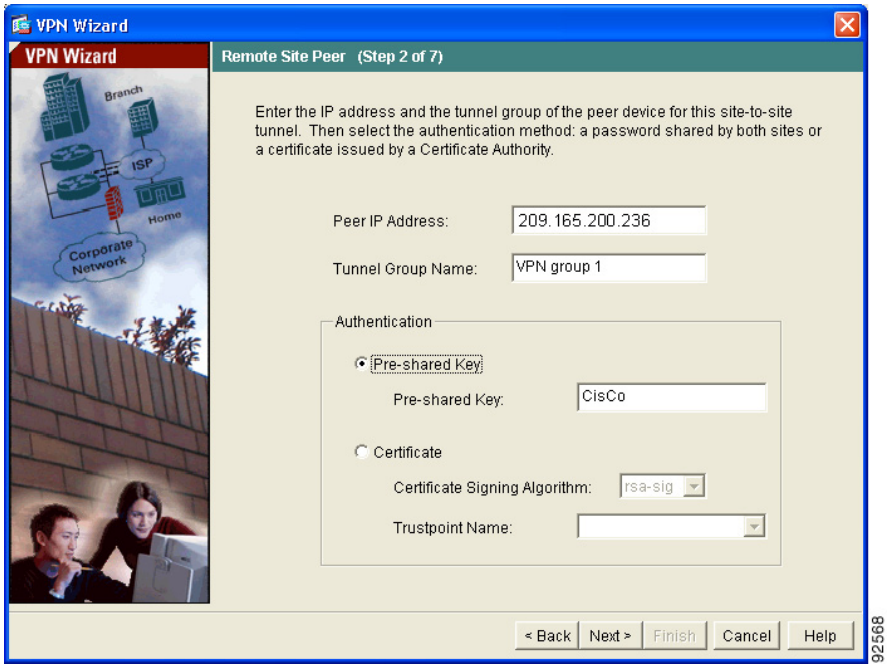
On page 2 of the VPN Wizard, provide information about the remote VPN peer. In this scenario, the remote VPN peer is ASA security appliance 2, from this point forward referred to as ASA 2. Perform the following steps:

1. Enter the Peer IP Address (ASA 2) and a Tunnel Group Name.

2. Specify the type of authentication that you want to use by performing one of the following steps:
   - To use a pre-shared key for authentication (for example, "CisCo"), click the **Pre-Shared Key** radio button, and enter a pre-shared key, which is shared for IPSec negotiations between both adaptive security appliances.

     Note When you configure the ASA 2 at the remote site, the VPN peer is ASA 1. Be sure to enter the *same* Pre-shared Key (CisCo) that you use here.

   - To use digital certificates for authentication instead, click the **Certificate** radio button, and then choose a Trustpoint Name from the drop-down menu.



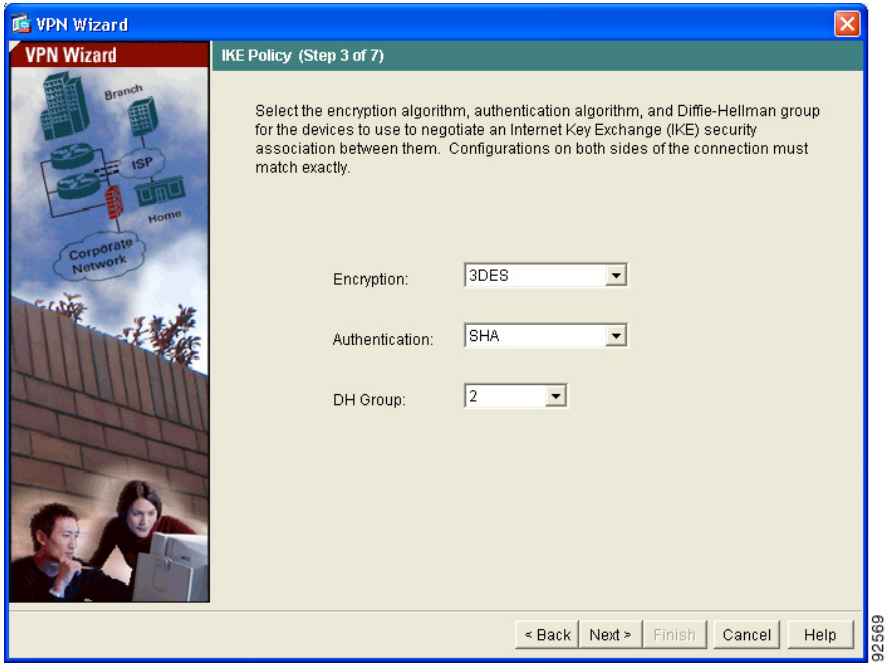
3. Click **Next** to continue.

Step 3: Configure the IKE Policy.

IKE is a negotiation protocol that includes an encryption method to protect data and ensure privacy; it is also an authentication method to ensure the identity of the peers. In most cases, the ASDM default values are sufficient to establish secure VPN tunnels between two peers.

To specify the IKE policy, perform the following steps:

1. Select the Encryption (DES/3DES/AES), authentication algorithms (MD5/SHA), and the Diffie-Hellman group (1/2/5) used by the adaptive security appliance during an IKE security association.

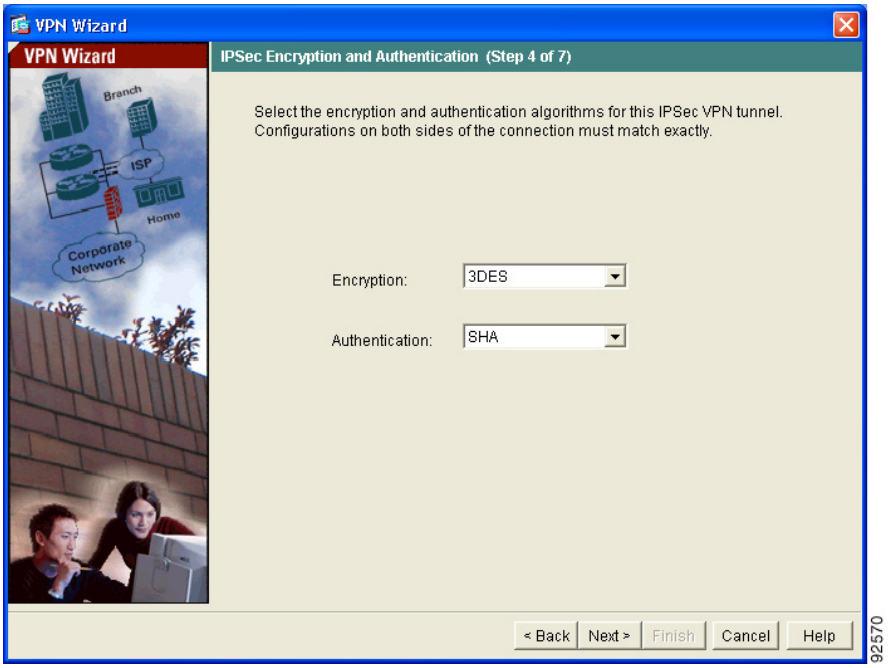


Note When configuring ASA 2, enter the exact values for each of the options that you chose for ASA 1. Encryption mismatches are a common cause of VPN tunnel failures and can slow down the process.

2. Click **Next** to continue.

Step 4: Configure IPSec Encryption and Authentication parameters.

1. Choose the Encryption algorithm (DES/3DES/AES) and authentication algorithm (MD5/SHA).



2. Click **Next** to continue.

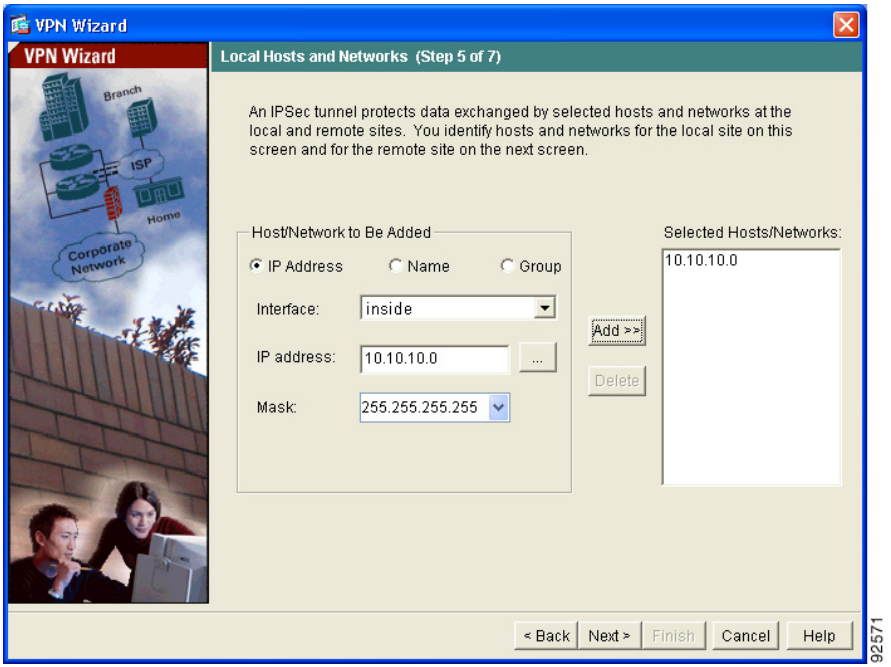
Step 5: Specify Local Hosts and Networks.

Identify hosts and networks at the local site to be allowed to use this IPSec tunnel to communicate with the remote-site peers. (The remote-site peers will be specified in a later step.)

On page 5 of the VPN Wizard, add or remove hosts and networks dynamically by clicking on **Add** or **Delete** respectively. In the current scenario, traffic from Network A (10.10.10.0) is encrypted by SA 1 and transmitted through the VPN tunnel.

On page 5 of the VPN Wizard, specify a local host or network to be allowed access to the IPSec tunnel. Perform the following steps:

1. Click **IP Address**.
2. Specify whether the interface is **inside** or **outside** by choosing an interface from the drop-down menu.
3. Enter the IP address and mask.
4. Click **Add**.
5. Repeat Steps 1 through Step 5 for each host or network that you want to have access to the tunnel.



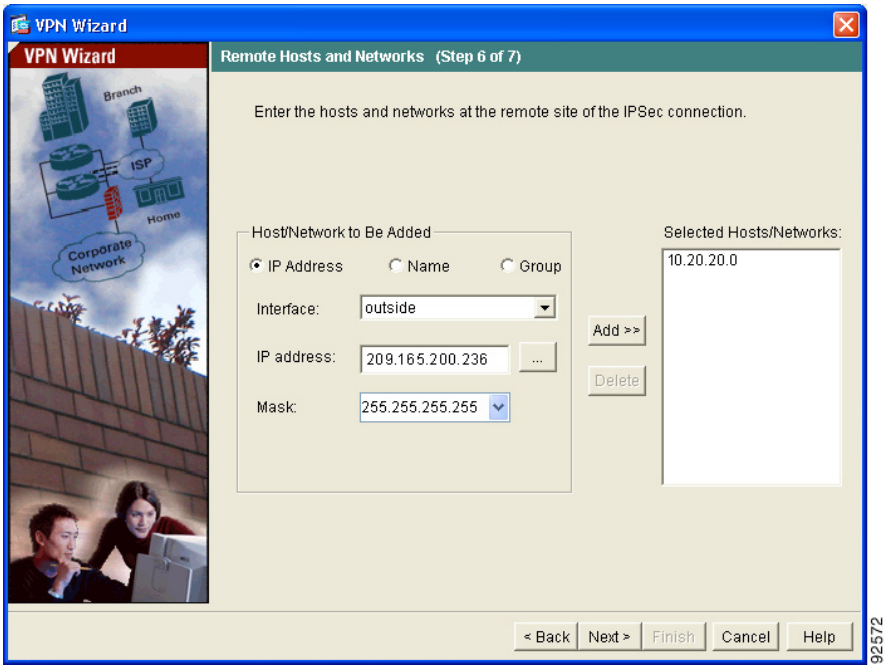
6. Click **Next** to continue.

Step 6: Specify Remote Hosts and Networks.

Identify hosts and networks at the remote site to be allowed to use this IPSec tunnel to communicate with the local hosts and networks you identified in Step 5. Add or remove hosts and networks dynamically by clicking **Add** or **Delete** respectively. In the current scenario, for ASA 1, the remote network is Network B (10.20.20.0), so traffic encrypted from this network is permitted through the tunnel.

To specify a remote host or network to be allowed access to the IPSec tunnel, perform the following steps:

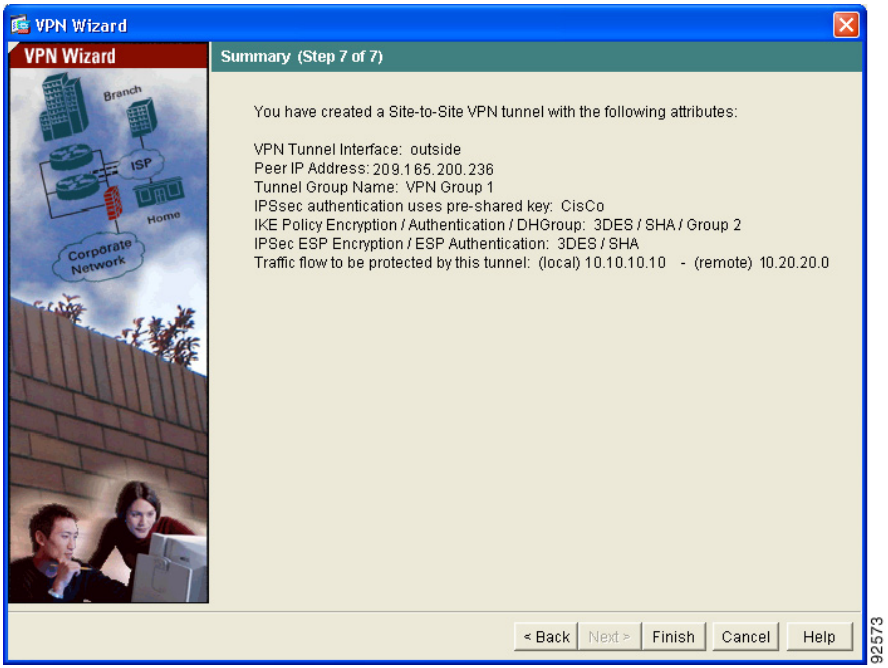
1. Click **IP Address**.
2. Specify whether the interface is **inside** or **outside** by choosing one interface from the **Interface** drop-down menu.
3. Enter the IP address and mask.
4. Click **Add**.
5. Repeat Step 1 through Step 5 for each host or network that you want to have access to the tunnel.



6. Click **Next** to continue.

Step 7: View VPN Attributes and Complete Wizard.

Review the configuration list for the VPN tunnel you just created. If you are satisfied with the configuration, click **Finish** to apply the configuration changes to the adaptive security appliance.


VPN Wizard
VPN Wizard
Summary (Step 7 of 7)
Branch
ISP
Home
Corporate Network
You have created a Site-to-Site VPN tunnel with the following attributes:
VPN Tunnel Interface: outside
Peer IP Address: 209.165.200.236
Tunnel Group Name: VPN Group 1
IPSsec authentication uses pre-shared key: CisCo
IKE Policy Encryption / Authentication / DHGroup: 3DES / SHA / Group 2
IPSec ESP Encryption / ESP Authentication: 3DES / SHA
Traffic flow to be protected by this tunnel: (local) 10.10.10.10 - (remote) 10.20.20.0
< Back
Next >
Finish
Cancel
Help
92573

This concludes the configuration process for ASA 1.

What to Do Next

You have just configured the local adaptive security appliance. Now you need to configure the adaptive security appliance at the remote site.

At the remote site, configure the second adaptive security appliance to serve as a VPN peer. Use the procedure you used to configure the local adaptive security appliance, starting at *Step 1: Configure the adaptive security appliance at the first site* on page 36, and finishing with *Step 7: View VPN Attributes and Complete Wizard* on page 43.

Note When configuring ASA 2, enter the exact same values for each of the options that you selected for ASA 1. Mismatches are a common cause of VPN configuration failures.

5 Optional SSM Setup and Configuration Procedures

The adaptive security appliance supports optional security service modules (SSMs) that plug into the chassis and provide additional functionality. This section describes setup and configuration procedures for the 4GE SSM and the AIP SSM.

4GE SSM Procedures

The 4GE Security Services Module (SSM) has eight Ethernet ports: four 10/100/1000 Mbps, copper, RJ-45 ports and four 1000 Mbps, small form-factor pluggable (SFP) fiber ports. You can mix the copper and fiber ports using the same 4GE card.

If you purchased a 4GE SSM, use the procedures in this section to:

- Cable the interfaces you want to use.
- Change the media type setting for any SFP interfaces you want to use.

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for any Ethernet interfaces you use.

Step 1: Cabling 4GE SSM Interfaces

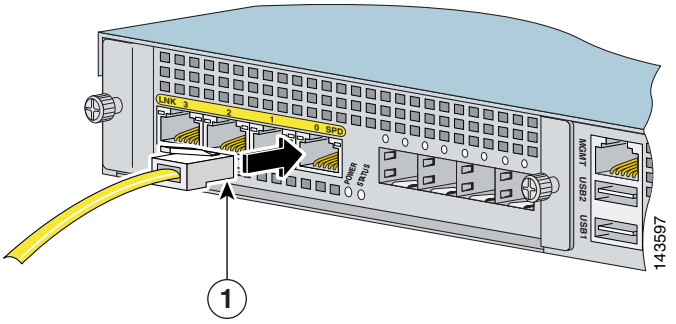
To cable 4GE SSM interfaces, perform the following steps for each port you want to connect to a network device:

Step 1 To connect an RJ-45 (Ethernet) interface to a network device, perform the following steps for each interface:

a. Locate a yellow Ethernet cable from the accessory kit.

b. Connect one end of the cable to an Ethernet port on the 4GE SSM.

Figure 7 Connecting the Ethernet port



1	RJ-45 (Ethernet) port

c. Connect the other end of the cable to your network device.

Step 2 (Optional) If you want to use an SFP (fiber optic) port, install and cable the SFP modules as shown in Figure 8:

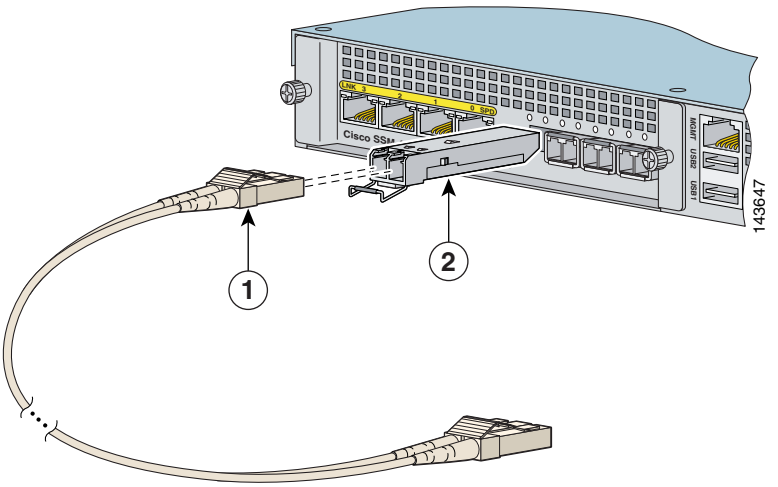
a. Insert and slide the SFP module into the SFP port until you hear a click. The click indicates that the SFP module is locked into the port.

b. Remove the optical port plugs from the installed SFP.

a. Locate the LC connector (fiber optic cable) in the 4GE SSM accessory kit.

b. Connect the LC connector to the SFP port.

Figure 8 Connecting the LC Connector



1	LC connector	**2**	SFP module

c. Connect the other end of the LC connector to your network device.

After you have attached any SFP ports to your network devices, you must also change the media type setting for each SFP interface. Continue with the following procedure, "Step 2: (Optional) Setting the 4GE SSM Media Type for Fiber Interfaces."

Step 2: (Optional) Setting the 4GE SSM Media Type for Fiber Interfaces

For each SFP interface, you must change the media type setting from the default setting (Ethernet) to Fiber Connector.

Note Because the default media type setting is Ethernet, you do not need to change the media type setting for Ethernet interfaces you use.

To set the media type for SFP interfaces using ASDM, perform the following steps starting from the main ASDM page:

Step 1 Click **Configuration**, at the top of the ASDM window.

Step 2 Choose the **Interfaces** feature on the left side of the ASDM window.

Step 3 Choose the 4GE SSM interface and click **Edit**. The Edit Interface dialog box appears.

Step 4 Click **Configure Hardware Properties**. The Hardware Properties dialog box appears.

Step 5 Click the **Media Type** drop-down menu and choose **Fiber Connector**.

Step 6 Click **OK** to return to the Edit Interfaces dialog box, then click **OK** to return to the interfaces configuration dialog box.

Step 7 Repeat this procedure for each SFP interface.

You can also set the media type from the command line. For more information, see *Configuring Ethernet Settings and Subinterfaces* in the *Cisco Security Appliance Command Line Configuration Guide*.

AIP SSM Procedures

The optional AIP SSM runs advanced IPS software that provides further security inspection either in inline mode or promiscuous mode. The security appliance diverts packets to the AIP SSM just before the packet exits the egress interface (or before VPN encryption occurs, if configured) and after other firewall policies are applied. For example, packets that are blocked by an access list are not forwarded to the AIP SSM.

If you purchased an AIP SSM, use the procedures in this section to:

- Cable the management interface
- Configure the adaptive security appliance to identify traffic to be diverted to the AIP SSM
- Session into the AIP SSM and run setup

Because the IPS software that runs on the AIP SSM provides many features and is beyond the scope of this document, detailed configuration information is available in the following separate documentation:

- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Cisco Intrusion Prevention System Command Reference*

Step 1: Cabling the AIP SSM Management Interface

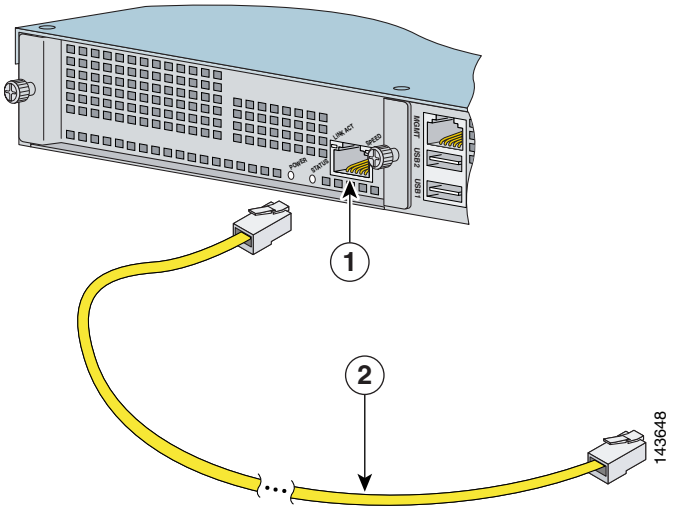
To cable the AIP SSM management interface, perform the following steps:

Step 1 Locate a yellow Ethernet cable from the accessory kit.

Step 2 Connect one end of the cable to the management port on the AIP SSM, as shown in Figure 9.

Step 3 Connect the other end of the cable to your network device.

Figure 9 Connecting to the Management Port



1	Management port	**2**	RJ-45 to RJ-45 cable

Step 2: Configuring the ASA 5500 to Divert Traffic to the AIP SSM

To specify the traffic that should be diverted from the security appliance to the AIP SSM, perform the following steps:

Step 1 To specify the traffic to be diverted to the AIP SSM, add a class map using the **class-map** command. For more information, see *Using Modular Policy Framework* in the *Cisco Security Appliance Command Line Configuration Guide*.

Step 2 To add or edit a policy map that sets the actions to take with the class map traffic, enter the following command:

```
hostname(config)# policy-map name
```

Step 3 To identify the class map from Step 1 to which you want to assign an action, enter the following command:

```
hostname(config-pmap)# class class_map_name
```

Step 4 To assign traffic to the AIP SSM, enter the following command:

```
hostname(config-pmap-c)# ips {inline | promiscuous} {fail-close | fail-open}
```

Where the **inline** keyword places the AIP SSM directly in the traffic flow. No traffic can continue through the security appliance without first passing through, and being inspected by, the AIP SSM. This mode is the most secure because every packet is analyzed before being allowed through. Also, the AIP SSM can implement a blocking policy on a packet-by-packet basis. This mode, however, can affect throughput.

The **promiscuous** keyword sends a duplicate stream of traffic to the AIP SSM. This mode is less secure, but has little impact on traffic throughput. Unlike inline mode, the AIP SSM can only block traffic by instructing the security appliance to **shun** the traffic or by resetting a connection on the security appliance. Moreover, while the AIP SSM is analyzing the traffic, a small amount of traffic might pass through the security appliance before the AIP SSM can block it.

The **fail-close** keyword sets the security appliance to block all traffic if the AIP SSM is unavailable.

The **fail-open** keyword sets the security appliance to allow all traffic through, uninspected, if the AIP SSM is unavailable.

Step 5 To activate the policy map on one or more interfaces, enter the following command:

```
hostname(config)# service-policy policymap_name {global | interface
interface_name}
```

Where **global** applies the policy map to all interfaces, and **interface** applies the policy to one interface. Only one global policy is allowed. You can override the global policy on an interface by applying a service policy to that interface. You can only apply one policy map to each interface.

The following example diverts all IP traffic to the AIP SSM in promiscuous mode, and blocks all IP traffic should the AIP SSM card fail for any reason:

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
```

```
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ids-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

Step 3: Sessioning to the AIP SSM and Running Setup

After you have completed configuration of the ASA 5500 series adaptive security appliance to divert traffic to the AIP SSM, session to the AIP SSM and run the setup utility for initial configuration.

Note You can either session to the AIP SSM from the adaptive security appliance (by using the session 1 command) or you can connect directly to the AIP SSM using SSH or Telnet on its management interface. Alternatively, you can use ASDM.

To session to the AIP SSM from the adaptive security appliance, perform the following steps:

Step 1 Enter the **session 1** command to session from the ASA 5500 series adaptive security appliance to the AIP SSM.

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

Step 2 Enter the username and password. The default username and password are both cisco.

Note The first time you log in to the AIP SSM you are prompted to change the default password. Passwords must be at least eight characters long and not a dictionary word.

```
login: cisco
Password:
Last login: Fri Sep  2 06:21:20 from xxx.xxx.xxx.xxx
***NOTICE***
This product contains cryptographic features and is subject to United States and
local country laws governing import, export, transfer and use. Delivery of Cisco
cryptographic products does not imply third-party authority to import, export,
distribute or use encryption. Importers, exporters, distributors and users are
responsible for compliance with U.S. and local country laws. By using this product
you agree to comply with applicable laws and regulations. If you are unable to
comply with U.S. and local laws, return this product immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to
```

```
export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
AIP SSM#
```

Note If you see this license notice (which appears only in some versions of the software), you can ignore the message until you need to upgrade the signature files on the AIP SSM. The AIP SSM continues to operate at the current signature level until a valid license key is installed. You can install the license key at a later time. The license key does not affect the current functionality of the AIP SSM.

Step 3 Enter the **setup** command to run the setup utility for initial configuration of the AIP SSM.

```
AIP SSM# setup
```

What to Do Next

You are now ready to configure the AIP SSM for intrusion prevention. See the following guides for AIP SSM configuration information:

- *Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*
- *Cisco Intrusion Prevention System Command Reference*

6 Optional Maintenance and Upgrade Procedures

Obtaining DES and 3DES/AES Encryption Licenses

The adaptive security appliance offers the option to purchase a DES or 3DES-AES license to enable specific features that provide encryption technology, such as secure remote management (SSH, ASDM, and so on), site-to-site VPN, and remote access VPN. Enabling the license requires an encryption license key.

If you ordered your adaptive security appliance with a DES or 3DES-AES license, the encryption license key comes with the adaptive security appliance.

If you did not order your adaptive security appliance with a DES or 3DES-AES license and would like to purchase one now, the encryption licenses are available at no charge on Cisco.com.

If you are a registered user of Cisco.com and would like to obtain a DES or 3DES/AES encryption license, go to the following website:

http://www.cisco.com/cgi-bin/Software/FormManager/formgenerator.pl

If you are not a registered user of Cisco.com, go to the following website:

http://www.cisco.com/pcgi-bin/Software/FormManager/formgenerator.pl

Provide your name, e-mail address, and the serial number for the adaptive security appliance as it appears in the **show version** command output.

Note You will receive the new activation key for your adaptive security appliance within two hours (or less) of requesting the license upgrade.

For more information on activation key examples or upgrading software, see the *Cisco Security Appliance Command Line Configuration Guide*.

To use the activation key, follow these steps:

	Command	Purpose
Step 1	hostname# **show version**	Shows the software release, hardware configuration, license key, and related uptime data.
Step 2	hostname# **configure terminal**	Enters global configuration mode.

	Command	Purpose
Step 3	hostname(config)# **activation-key** *activation-5-tuple-key*	Updates the encryption activation key by replacing the *activation-4-tuple-key* variable with the activation key obtained with your new license. The *activation-5-tuple-key* variable is a five-element hexadecimal string with one space between each element. An example is 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e. The "0x" is optional; all values are assumed to be hexadecimal.
Step 4	hostname(config)# **exit**	Exits global configuration mode.
Step 5	hostname# **copy running-config startup-config**	Saves the configuration.
Step 6	hostname# **reload**	Reboots the adaptive security appliance and reloads the configuration.

Restoring the Default Configuration

You can restore your configuration back to the factory default values in one of the following ways:

- You can start the Startup Wizard at this URL: **https://192.168.1.1**.
- You can use the command line as specified in the following procedure.

To restore your default configuration back to the factory-default values, perform the following steps:

	Command	Purpose
Step 1	hostname# **configure factory-default** [*inside_IP_address* [*mask*]][1]	Erases the running configuration and replaces it with the factory default configuration.
Step 2	hostname# **write memory**	Writes the factory default configuration to Flash memory.

1. If the optional inside IP address and address mask are specified, the factory-default configuration reflects that.

See the *Cisco Security Appliance Command Line Configuration Guide* for detailed command information and configuration examples:

The Cisco TAC website is available to all customers who need technical assistance. To access the TAC website, go to this URL:

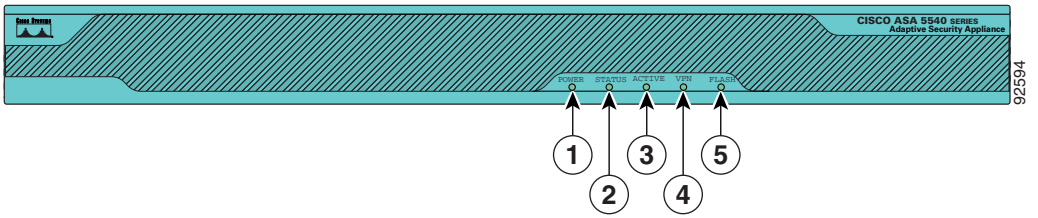
http://www.cisco.com/tac

Checking the LEDs

This section describes the front, rear, and the panel LEDs for the adaptive security appliance.

Figure 10 shows the front view of the adaptive security appliance.

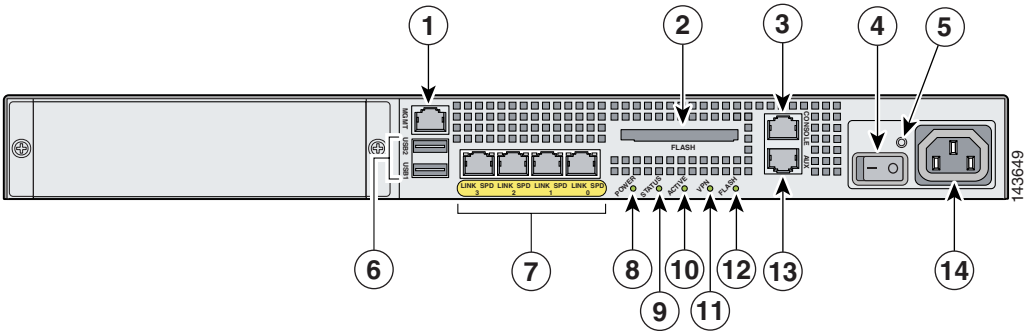
Figure 10 Cisco ASA 5540 Adaptive Security Appliance Front Panel Features



	LED	Color	State	Description
1	Power	Green	On	On when the adaptive security appliance has power.
2	Status	Green	Flashing	When the power-up diagnostics are running or the system is booting.
			Solid	Green when the system has passed power-up diagnostics.
		Amber	Solid	Amber when the power-up diagnostics have failed.
3	Active	Green	Flashing	When there is network activity.
4	VPN	Green	Solid	When data is passing through the interface.
5	Flash	Green	Solid	When the CompactFlash device is being accessed.

Figure 11 shows the rear panel features for the adaptive security appliance.

Figure 11 Cisco ASA 5540 Adaptive Security Appliance Rear Panel Features



1	MGMT	**8**	Power indicator
2	External CompactFlash device	**9**	Status indicator
3	Serial Console port	**10**	Active
4	Power switch	**11**	VPN
5	Power indicator light	**12**	Flash
6	USB 2.0	**13**	AUX ports
7	Network interfaces	**14**	Power connector

Figure 12 shows the adaptive security appliance rear panel LEDs.

Figure 12 Cisco ASA 5540 Adaptive Security Appliance Rear Panel LEDs

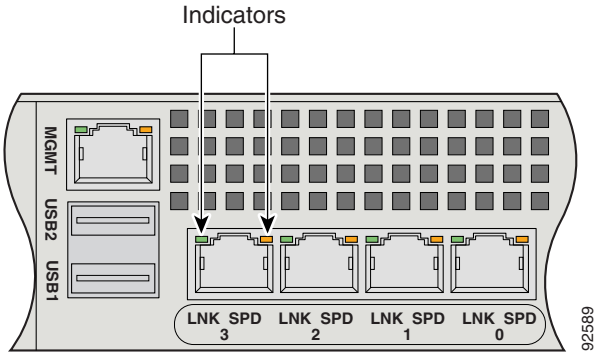


Table 1 lists the state of the adaptive security appliance rear panel LEDs.

Table 1 Rear Panel LEDs

Indicator	Color	Description
Left side	Solid Green	Physical Link
	Green Flashing	Network Activity
Right side	Not lit	10 Mbps
	Green	100 Mbps
	Amber	1000 Mbps

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.

- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is "down," or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expet logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

Printed in the USA on recycled paper containing 10% postconsumer waste.

78-16915-02
DOC-7816915=